INTERNAL AUDITOR

APRIL 2015

INTERNALAUDITOR.ORG

Deciphering Digital Signatures

Is Your Organization ACA Compliant?

The Internal Auditor as Professional Skeptic

Minimizing Joint Venture Risk

KNOWLEDGE SHARING

Small audit functions can learn a lot about best practices from their larger counterparts, and vice versa.

Ms. Mona Hussain
Head of Internal Audit
Dubai World Trade Centre
United Arab Emirates

dwtc.com

"IDEA® has provided us with an all-in-one solution enabling greater reliability and comprehensiveness of analysis and results. Without doubt, through time saved during the audit process alone, I can say that CaseWare IDEA has produced a clear return on investment for our business."

CaseWare ANALYTICS

PRINCIPAL PARTNER

casewareanalytics.com | sales@caseware-idea.com

Crowe Horwath®

Relationships are built on many things...

Like having partners involved on your account.

Our clients experience the value of Crowe Horwath LLP professionals who understand their business and offer valuable insights relevant to the challenges they face.

The internal audit function can contribute more to an organization than many realize. But if it is to be recognized as an important strategic player, an organization's internal audit department must expand its role and align its contributions with organizational objectives.

To learn more about how you can become a strategic player, visit crowehorwath.com/risk and download our article, "Making Internal Audit More Strategic, More Valuable," or contact Tony Klaich at 415.946.7447 or tony.klaich@crowehorwath.com.

Tony Klaich, Partner
Manufacturing and Distribution Risk Consulting Leader
San Francisco

Follow us.

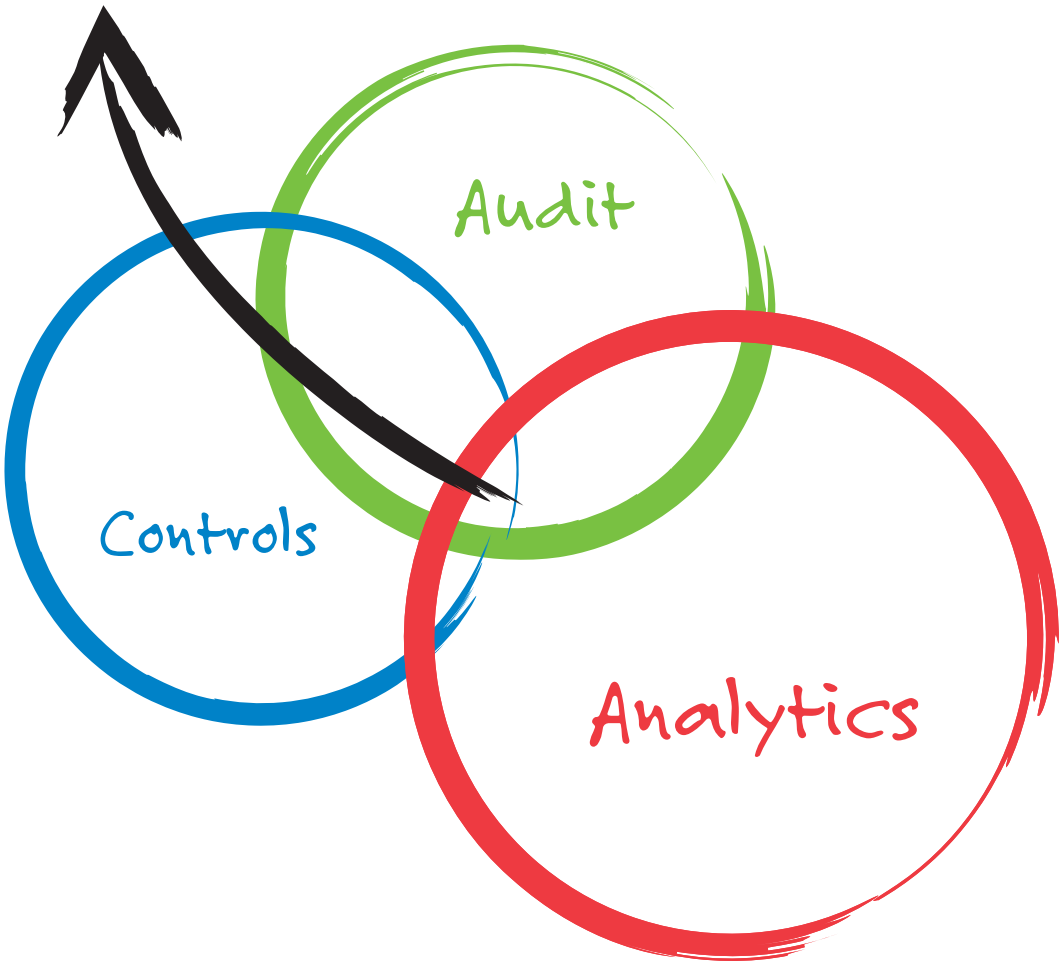
Audit | Tax | Advisory | Risk | Performance

The Unique Alternative to the Big Four®

The governance, risk, and compliance management solutions from Crowe are endorsed by the American Bankers Association (ABA) through its subsidiary, the Corporation for American Banking. The ABA endorsement of these solutions indicates they deliver high quality and meet performance standards, and offer the potential to improve your bank's profitability and performance.

TeamMate®

Ecosystem for Audit



TeamMate Analytics - Data Analysis for Every Audit

TeamMate Analytics includes more than 150 audit tools and runs on top of Excel, allowing auditors to easily perform powerful data analysis and deliver significant value without the need for extensive training. TeamMate Analytics is a powerful standalone solution for any auditor, and is especially beneficial to those using TeamMate already.

TeamMate's Ecosystem for Audit offers comprehensive solutions for all of your organization's audit, controls, and data analytics requirements.

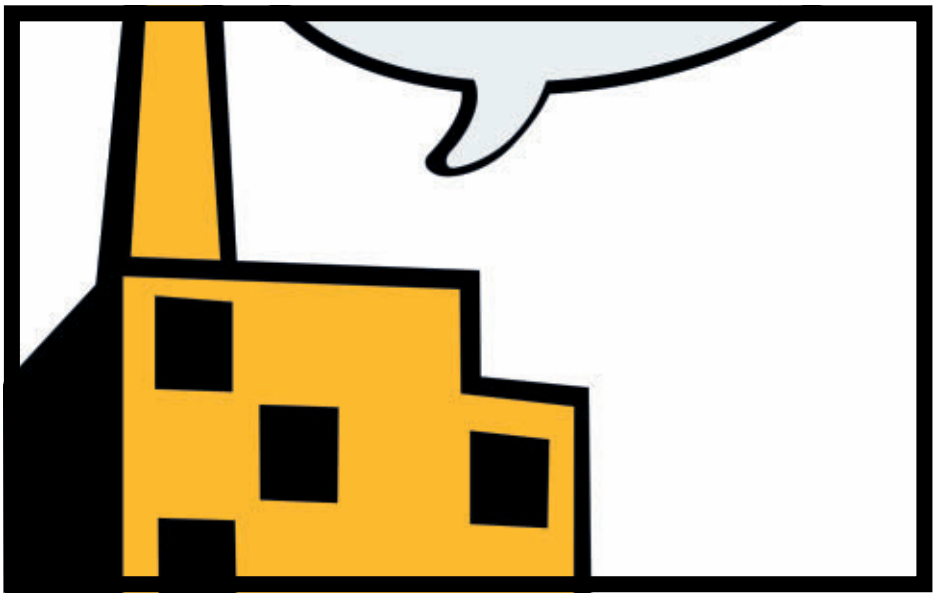
Start your free trial today at **TeamMateSolutions.com/Trial**

Wolters Kluwer
Audit, Risk & Compliance

PRINCIPAL PARTNER

Ia
INTERNAL AUDITOR

APRIL 2015 VOLUME LXXII: II



FEATURES

28 COVER **Small Audit Functions, Big Ideas** Audit departments of limited size can learn a lot from their larger counterparts, but they have much to teach as well. **ARTHUR PIPER**

35 Digital Signatures Deciphered Internal auditors should assess the business processes and risks associated with electronic signatures. **SHIVA HULLAVARAD, RUSSELL O'HARE, ASHOK ROY**

40 Untangling the ACA A smart approach to U.S. Affordable Care Act compliance begins with a comprehensive risk assessment. **RUSSELL A. JACKSON**

47 Reinventing Internal Audit Recent governance-related developments require the profession to revisit some of its long-held paradigms. **TIM J. LEECH**

52 Professional Skepticism The internal auditor's ability to approach an engagement objectively is influenced greatly by the skepticism exhibited. **REBEKAH A. HEATH AND TIM STAGGS**

57 Joint Venture/Joint Exposure An effective joint venture governance strategy can ensure an appropriate level of owner oversight and minimize shared risks. **BEN ARNOLD**

Audit Management & Data Analysis Software

Does this sound familiar?

- You spend most of your day managing spreadsheets, shared drives and email.
- You'd rather add value for your organization by showcasing material improvement and risk mitigation opportunities – not chasing after tick marks in e-documents.
- You'd love to easily report on strategic risks, recommendations, and remediation statuses – anytime senior management or the board asks.
- You'd feel much more confident if your recommendations and findings can be backed by quantifiable, data-based evidence.

---

acl™

Your audit management tool should do much more than manage workpapers

ACL GRC is the *only solution* that integrates robust data analytics with easy-to-use, cloud-based audit management software.

Turn Analysis into Actionable Results - Anytime, Anywhere.

Watch the video on acl.com/a-better-way to see how it works in less than 2 minutes.

INTERNAL AUDITOR

APRIL 2015 VOLUME LXXII: II

DEPARTMENTS

7 Editor's Note

9 Reader Feedback

PRACTICES

13 UPDATE Fraudsters eye mobile e-commerce; CFOs face reporting challenges; and executives fail to make information security a priority.

17 Back to Basics Good working relationships lead to effective engagements.

20 ITAudit Data visualization tools can be used to assess fraud risk.

22 Risk Watch Internal audit needs to consider the upside of risk.

25 Fraud Findings A fake CFO dupes an unsuspecting clerk.

INSIGHTS

62 Governance Perspectives Organizations should facilitate whistleblowing without fear.

65 The Mind of Jacka Three high-risk audits are often ignored.

66 Eye on Business Experts offer best practice advice for small audit functions.

68 In My Opinion A former auditor takes a hindsight view of his time in the profession.

ONLINE InternalAuditor.org

ACA Health Check Internal auditors in the health-care industry share their approaches to assessing risk around the U.S. Affordable Care Act.

Cyberrisk Top of Mind Internal audit professionals say management's engagement with cybersecurity correlates with the organization's ability to manage information security risks, a new report says.

Transformational Change In an exclusive video, Tim Leech, author of "Reinventing Internal Audit" (page 47), explains why the profession may need to revisit existing paradigms.

The Empty Boxes Scheme Art Stewart discusses lessons from the case of would-be distributors who were conned into paying US$13 million for nonexistent semiconductors.

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

THE CONTINUOUS AUDIT

In today's ever-evolving business environment, it is clear that internal auditors need to constantly align—and realign—their audit coverage to address emerging risks and avoid damaging surprises. But are audit functions up to the task?

The latest North American Pulse of Internal Audit report from The IIA's Audit Executive Center indicates they are—to an extent. More than half of the 311 CAE and audit management level respondents to the Pulse survey say internal audit's biggest challenge in continuously assessing risks is its ability to identify emerging risks and incorporate them into the audit plan. However, nearly 90 percent of respondents say their audit planning is designed to be responsive to changes in the organization's risk profile.

To be sure, 61 percent of respondents say their audit functions have the resources and expertise to assess risks continuously and analyze their potential impact to the business model. However, audit functions are waging a battle for talent, with 40 percent of those surveyed saying attracting and retaining talent is a high or critical priority.

The need for both a broader and deeper understanding of critical business issues comes across loud and clear in recent research by the ERM Initiative at North Carolina State University. According to the study, 59 percent of senior finance executives say the volume and complexity of risks facing their companies have changed "extensively" or "mostly" in the last five years. And 65 percent say their organization was caught off guard by at least one operational surprise "somewhat" or "extensively" during that time.

Continuous assessment of emerging risks can be more of a challenge for small internal audit departments than for larger, better-resourced functions. In our cover story, "Small Audit Functions, Big Ideas," author Arthur Piper looks at the practices some small audit departments implement to ensure they provide comprehensive, continual assessments of the risks facing the organization.

According to the Pulse report, geopolitical, macroeconomic, and cyber-related risks will put enormous pressure on many internal audit functions to raise their game. Given the significance of these emerging risks, it is imperative that internal audit functions be able to assess risk on a continuous basis. As the authors of the report state, "In today's fast-paced operating environments, internal auditors need to audit at the speed of risk."

Anne Millage

PREPARE TO PASS THE CIA® EXAM

With The IIA's CIA Learning System®.

With a busy and unpredictable schedule, finding the time to study for the Certified Internal Auditor® (CIA) exam can be difficult. Stay focused and take advantage of your downtime with The IIA's CIA Learning System.

Enjoy quality and convenience:

- Learn the entire global CIA exam syllabus in a concise and easy-to-understand format.
- Access your reading materials via your e-reader device.
- Create a customized SmartStudy™ plan based on your strengths and weaknesses.
- Study on-the-go with mobile-optimized online tools.

To create your free study plan, visit www.LearnCIA.com.

The Institute of Internal Auditors

142007

Reader Feedback

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.

Working With External Audit

I agree that internal audit is wise to collaborate and communicate with all stakeholders, including external audit. Here is another perspective for discussion: Wouldn't it be wonderful if internal audit could rely on the work of external auditors? If internal audit could be certain that external audit was performing the work it was engaged to perform—ensuring the integrity of financial statement reporting—internal audit could focus on the myriad other important responsibilities required under its professional standards, and risks of potentially even greater significance.

– Nancy *comments on Richard Turpen and Haley Dyer's "Working With External Auditors" ("Back to Basics," February 2015).*

I have doubts that today's internal auditor is focusing on saving audit fees as a primary objective. Yes, they need to be aware of the external auditors' plans, but hopefully they are instead focused on major risks to the organization. The authors used the word "collaboration," but I see the advice as being all about helping the external auditors. I don't see anything that the internal auditors are getting from the "collaboration."

– John Fraser *comments on Richard Turpen and Haley Dyer's "Working With External Auditors" ("Back to Basics," February 2015).*

We certainly agree with John that fee reduction is not the internal auditor's primary objective. As we emphasized in our article, internal audit addresses organizational risks beyond those normally of most concern to the external auditors. Achieving collaborative value starts with the auditor discussions we described, but true collaboration begins when those communications grow into an ongoing exchange of risk information.

– Richard Turpen *and* Haley Dyer

The Art of Internal Audit

In my opinion, CAEs should set the pace and encourage internal auditors to be more creative and innovative in their

Ia INTERNAL AUDITOR
APRIL 2015
VOLUME LXXII:II

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")

jobs. Status quos should be challenged in the process of internal auditing.

– Augustine Inogbo *comments on The Mind of Jacka blog post, "The Art of Internal Audit."*

Managing Risk

Risk management simply won't work well until the model defines what is "at risk" and provides that as context for the program. Management sees and manages purpose and objectives, not risk. So if we place risk in the context of what is already being managed, maybe risk management will take on meaning and value in the eyes of management.

– Daninmo *comments on the Marks on Governance blog post, "New Report Confirms the Failure of Risk Management Practices."*

Hear No Evil

As a profession, I think it's important we increasingly look at "delicate topics" such as this. An underlying psychological issue is that the issues you are referring to can raise a degree of anxiety in the minds of audit committee members.

– J. Paterson *comments on the Chambers on the Profession blog post, "Are There Things Audit Committees Would Rather Not Hear From Internal Audit?"*

Emerging Technologies

New technologies will emerge, we can all be assured of that. But we can also be assured that, with rare exceptions, no company will need to study, much less embrace, all new technologies. There must be a cost-benefit breakpoint in there. It might be more reasonable to be in the early majority rather than an early adopter so that, when one does study a new technology, there are some case studies and use analysis on which to base the decision. But that would not involve emerging technologies, but rather existing technologies. There is a risk, of course, in not being the first to market with a new technology. But that risk is partially mitigated by also not being the first to fail.

– Richard Fowler *comments on the Marks on Governance blog post, "The Risk of Missing the Next New Technology."*

VISIT InternalAuditor.org for the latest blogs

ideagen | Pentana

Pentana Analytics

Automated Testing and Continuous Monitoring now available within Pentana!

Powered by ARBUTUS

FREE Webinar

Register Today at www.ideagenplc.com/pentana

Ideagen have worked together with audit analytics software developer, Arbutus Software, to create the best of breed analytics solution to fully support your audit testing and to provide a continuous monitoring solution. The results are directly uploaded to Ideagen's audit and risk management solution, Pentana, along with any supporting evidence!

If you use a different analytics tool, do not worry! We can integrate our audit management solution, Pentana with other analytics tools also - enabling you to still benefit from automated testing and continuous monitoring.

About Ideagen's Pentana Solution

Pentana is a leading audit management solution, developed using the latest Microsoft technologies to empower internal audit departments to save essential time, increase efficiencies and maximize the power of collaborative working. It integrates all aspects of the audit cycle from annual planning to detailed risk assessment and controls testing, through to action tracking and Audit Committee reporting.

Key Benefits:

- Implements a consistent methodology compliant with international risk and auditing standards
- Simplifies global deployment with installation from a website and automatic updates downloaded without user intervention
- Optimizes performance for use over a wide range of network speeds as well as working off-line to provide a true global working environment for GRC professionals
- Pentana can equally be used for Enterprise Risk Management, SOX compliance, investigations, Health and Safety or any application where risk assessment and centralized action tracking are required

Don't just take our word for it! Visit our website www.ideagenplc.com/pentana to discover first-hand video case studies from our happy customers. Examples include, BBVA, BDO & Heineken.

CFOs' stakeholder balancing act... Audit committees complain of overload... Assessing reputation risk... IT questions executives' cybersecurity priorities.

Update

THE HIGH COST OF MOBILE COMMERCE

Companies report that fraud is chipping into a significant portion of their mobile-based revenue.

Mobile commerce fraud costs large and midsized businesses an average of US$92.3 million in revenue annually, according to a recent survey. For some, the amount comprises a revenue loss of up to 25 percent.

Mobile E-commerce: Friend or Foe? — a J. Gold Associates research report sponsored by information security vendor RSA and mobile identity provider Telesign — surveyed 250 companies with average revenues of US$2.54 billion. Among these firms, nearly half say they experienced between one and 24 overall fraud incidents in the past year, while one-fourth indicated they experienced between 25 and 250. For almost a third of respondents, between 10 percent and 24 percent of the incidents were mobile-based.

"With the shift to mobile e-commerce well underway, we know that hackers and fraud are never far behind," says Telesign CEO Steve Jillings. He notes that respondents expect mobile revenues to grow 47 percent over the next few years. "This represents a green field for fraud incidents if security postures remain the same."

Among mobile threats, respondents indicate that device malware represents the

CEOS SOUND OFF

Business leaders worldwide describe the challenges they face in an era of unprecedented change.

81% see mobile technologies as strategically important

78% are concerned about overregulation

61% are worried about cybersecurity

51% plan strategic alliances/joint ventures over the next 12 months

39% are very confident about their company's growth prospects

Source: PricewaterhouseCoopers 18th Annual Global CEO Survey

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

largest risk to their business, followed by e-wallet fraud and app store fraud. Fake mobile apps—apps masquerading as something else or embedded with malware—are also ranked as one of the top mobile device threats. Account takeover and password guessing were cited, as well.

Survey respondents also shared the type of mobile authentication they use. More than three-fourths rely on user names and passwords, and just over half use device IDs. Moreover, 44 percent report using challenge-based questions, while another 41 percent say they use IP recognition. Biometrics was identified as an up-and-coming priority, with nearly half citing it as a type of authentication they will require in the future. **– D. SALIERNO**

52%
OF CAES AND INTERNAL AUDIT DIRECTORS
in North America consider identifying emerging risks to be their biggest challenge for 2015.

37%
SAY THEY ARE JUST "MODERATELY CONFIDENT"
in their ability to assess risk on an ongoing basis.

"In today's operating environment, internal auditors have a clear mandate to identify and address major risks on a continual basis," says IIA President and CEO Richard Chambers.

Source: The IIA Audit Executive Center, 2015 Pulse of Internal Audit

PRESSURE MOUNTING

Diverse investors, regulatory requirements make it difficult for CFOs to satisfy the needs of all.

Seventy percent of chief financial officers (CFOs) find it challenging to balance the needs between corporate reporting requirements and stakeholder demands, according to Connected Reporting, a survey from EY's Financial Accounting and Advisory Services (FAAS).

Of the 500 CFOs and heads of reporting surveyed across Africa, the Americas, Asia-Pacific, Europe, India, and the Middle East, 97 percent face challenges to improve reporting, which includes cost and time to produce reports. Only 20 percent of respondents say their current reporting is highly effective in meeting external stakeholder needs.

Neri Bukspan, EY's financial reporting and disclosure leader, and a contributor to the report, says investors want to understand both where the company is now and where it wants to be in the future. "They want more information about strategy," he says. "They want to understand more about risks, and not necessarily just about the risks themselves, but about how they are being managed. These risks are not only financial risks, they could also include operational risk, cybersecurity, and others, none of which you would expect to find in a financial report."

While regulatory requirements call for highly detailed reports with a high degree of data accuracy to fixed timetables, investors may want more frequently accessible, short-format information on key performance indicators. **– S. STEFFEE**

IT'S A TOUGH JOB

Audit committee members say their workload has grown and extends beyond their financial expertise.

Even audit committee members complain of overwork, according to a survey by KPMG's Audit Committee Institute (ACI). In the 2015 Global Audit Committee Survey of 1,500 audit committee members, three-fourths say their oversight duties take more time, and half say the work has become more difficult. In addition to their traditional financial reporting oversight role, many audit committees now have some responsibility over cybersecurity, technology, compliance, and operational risks, the survey reports.

"The resounding message is that the audit committee can't do it all," ACI Executive Director Dennis Whalen says. "The risk environment is clearly straining many audit committee agendas today."

Some audit committee members are embracing the new realities of their position. Survey respondents say they want to devote more time on the committee's agenda to risk management

processes, operational risk, cybersecurity, and changing technologies. Cybersecurity and technology changes are among the risk areas for which respondents say they want better quality information, along with talent management, growth and innovation, and potential disruptors to the company's business model. Moreover, respondents say their interaction with the chief information and risk officers needs the most improvement.

In a letter responding to a recent *Wall Street Journal* article about audit committee workloads, IIA President and CEO Richard Chambers acknowledged the need for audit committee members to take on additional responsibilities. "Risks evolve, and any audit committee that resists venturing beyond its comfort zone does a disservice to the organization and its shareholders," he wrote.

Even so, many boards are giving audit committees some relief. The KPMG survey reports that 35 percent of organizations have reassigned some of the audit committee's nonfinancial oversight duties to the full board or to other committees. Another 32 percent of organizations may do so next year. "A lighter risk agenda for the audit committee can translate into more time for quality discussions and a deeper understanding of the business," Whalen says.
– T. MCCOLLUM

PRESERVING THE COMPANY BRAND

Internal audit should have a front seat in assessing the organization's reputational risk, says Sharon Grant, vice president of customer contact and former managing director at United Airlines.

As a long-time airline employee, what have you learned about addressing reputational risk? You must be quick to learn, admit mistakes, improve, and evolve. In today's environment, every experience is lived, felt, and shared on social media. A high level of active engagement is needed to ensure that if we make mistakes, we are quick to fix them. This is a responsibility of everyone in the organization, and the accountability for owning the management of these risks is important to preservation of the company's brand. Internal audit can serve a vital role in driving high accountability.

What should internal auditors do to assess reputational risk? Maintain credibility by being completely objective. Foundationally, internal auditors should be continually advancing, broadening, and elevating their skills to understand the threats the environment could have on reputation. Tactically, internal auditors should assess the current risk management structure and evaluate the specificity by which risk to reputation is built into the design of controls, as well, in the reporting of the effectiveness of business functions. Because of their objectivity, internal auditors are well-positioned to harness data and analytics to add value to the reputational-risk assessment process.

CYBER DISCONNECT

CISOs say executives don't make information security a priority.

Organizations are failing to address cybersecurity risks because chief information security officers (CISOs) and senior management aren't on the same page about such threats, says a Ponemon Institute study commissioned by Raytheon. Seventy-eight percent of respondents to the Global Megatrends in Cybersecurity 2015 survey say their organization's board hasn't been briefed about its cybersecurity strategy within the past year, while two-thirds say top executives haven't made information security a priority. Ponemon surveyed more than 1,000 CISOs and other senior IT leaders for the report.

That disconnect at the top is reflected in CISOs' lack of confidence in their organization's cybersecurity readiness. Less than half (47 percent) say their organization has the resources needed to meet information security requirements, and the same percentage say their organization complies with security standards. Two-thirds report their organization needs more qualified cybersecurity personnel to keep up with the growing risks. "Security leaders lack both funding and manpower to adequately protect assets and infrastructure," Ponemon Chairman Larry Ponemon says.

The report details seven cybersecurity trends facing organizations. One key trend is that although three-fourths of survey respondents say their organization's senior leaders view cybersecurity as a necessary cost, rather than a competitive advantage, a Ponemon panel of information security experts predicts that executives will see it as a competitive advantage three years from now. **– T. MCCOLLUM**

Back to Basics

BY JARED SOILEAU + LAURA SOILEAU EDITED BY JAMES ROTH

BUILDING RAPPORT

Good working relationships with audit clients can ensure effective engagements.

One of the keys to a successful internal audit is building rapport with the audit client. While there are many tools and techniques related to building rapport in the general sense, internal auditors can take actions throughout the course of their audit procedures to build relationships with their clients that will aid in maximizing the success of the internal audit function. These actions include understanding the business, active listening, maintaining respect for the client's time, a problem-solving attitude, and a partnering approach to the relationship.

Understanding the Business

Audit clients often will have more respect for internal auditors who demonstrate an understanding of the business or process that is being audited. Taking time to appropriately plan for client interactions, including reviewing prior audit workpapers and financial statements, understanding trends and key performance metrics for the area being audited, and understanding the regulatory environment are all ways to demonstrate an understanding of the business. Auditors should consider discussing any questions they have about the client's business with their management team in advance of client interactions to address any areas of uncertainty. Less experienced auditors also may consider including more experienced auditors in client meetings based on the knowledge level of the auditor and the information to be discussed.

Active Listening

There are numerous barriers to listening that can prevent auditors from truly understanding the message being relayed by the client. For example, lack of interest, bias, external or internal distractions, time constraints, and focusing on the next question to be asked can all limit an auditor's ability to interpret the information being communicated. To increase rapport with the client, internal auditors should approach meetings, interviews, and other interactions with the goal of active listening. A first step in this process is awareness of the barriers to active listening, and planning meetings with the intent of minimizing such barriers and limiting distractions. In some situations, this could include involving another team member in the meeting to take on the role of scribe. The auditor may also consider paraphrasing what the client said back to the client to ensure an accurate understanding of process, concerns, and information conveyed.

Respect for the Client's Time

Like anyone else, audit clients typically have many demands for their time. Demonstrating a respect for the client's

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

Incisive: A New Approach to Spreadsheets

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

Unmatched Visibility • Exceptional Control • Ease of Use

Learn more about spreadsheet risk management at incisive.com

300 Santana Row, Suite 200, San Jose, CA 95128
408.660.3090 | www.incisive.com

incisive™

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

ELEMENTS OF RAPPORT

Building an effective working relationship with clients can facilitate communication and help practitioners produce more meaningful audit results. Several key actions, in particular, go a long way toward establishing client rapport.

time through planning in advance of the audit process, proactive communication, advanced scheduling of meetings, arriving to meetings and other appointments on time, and keeping to scheduled meeting times and agenda items (as applicable) will provide an opportunity for the internal auditor to further build rapport with his or her audit clients. Further, auditors should consider turning their cell phone ringer off and avoid looking at the phone during meetings with the client. In addition, to the extent possible, auditors should confirm their information request list is comprehensive to minimize the back and forth with the client. Finally, the auditor should evaluate the form of communication to ensure it is not only best suited to client preferences but that it is also the most effective method of communication to obtain necessary information. This may involve having a conversation with the client at the outset of the audit to identify and understand the client's communication preferences.

Problem-solving Attitude

Auditors should approach each internal audit with a focus on not only understanding the internal and external environment of the operating unit, but also with an intent to peel back the layers of the information gathered, including any exceptions identified to understand the who, what, when, where, why, and how behind the information. Through this process, the auditor may identify risks that were not considered in prior audits. To maximize the effectiveness of the audit, auditors should team with the client to identify the most appropriate solutions for any risks or issues that are uncovered.

Partnering

Historically, internal auditors have had a negative reputation in some organizations due to a "gotcha" attitude. Further, in some organizations internal auditors have been seen as the "police," reporting back to management all of the things that an operating unit is doing wrong. Internal auditors have an opportunity to build rapport with, and gain respect from, their audit clients by developing a partnering approach to the relationship. This can include working hand-in-hand with the client to truly understand the root causes behind any issues identified and working toward recommendations that not only address the root cause but also consider the associated benefits and costs. This can incorporate reporting to upper management any best practices the client has implemented within its organization and sharing best practices that the auditor has seen within other operating units.

Adding Value

Building rapport with the audit client should not only make the day-to-day audit process more enjoyable for the internal auditor and the client, but ideally, it also will lead to a more successful internal audit function that will add maximum value to clients. While these actions may appear to be common sense, keeping them front of mind during interactions with the client should result in a more positive experience for all parties involved in the audit process.

JARED SOILEAU, CIA, CRMA, CISA, *is an assistant professor of accounting at Louisiana State University in Baton Rouge.*
LAURA SOILEAU, CIA, CRMA, CPA, *is an associate director in Postlethwaite & Netterville's Consulting Department in Baton Rouge.*

BY STEVE MAR

GET A VIEW INTO SUSPICIOUS TRANSACTIONS

Data visualization tools can help internal auditors dig deep to uncover potential fraud.

The U.S. Centers for Medicare and Medicaid Services' June 2014 Report to Congress on Medicare's Fraud Prevention System (FPS) describes how the state-of-the-art predictive analytics system identified US$210 million in savings during its second year of operation. The FPS' ability to identify savings illustrates the power of data analytics to detect suspicious transactions.

Internal audit can leverage analytics technologies to audit for similar transactions within their organization. Data visualization is an analytic tool that can allow auditors to rapidly interrogate an entire transaction history or database to identify the most suspicious transactions to investigate.

A Fraud Risk Tool

The internal audit department at one Fortune 500 company applied data visualization tools to a project to assess fraud risk. The first phase of the risk assessment identified several high-risk scenarios such as processing duplicate payments, paying invoices for the same purchases, and submitting payments to false vendors. In the second phase, the review team deployed a data visualization tool to the existing data sets.

The first step involved planning and setting specific project-review objectives. The review team interviewed key process stakeholders to learn the financial process flow and studied the database structure and data dictionary. For this specific database, the team collected 700,000 transactions for a 12-month period.

Once the review team had loaded the transaction data into a data analytics software tool, it began the time-consuming job of cleansing and normalizing the data to support the project objectives. The data came in four different files and required three iterations to eliminate any false positives and meaningless data, as well as to provide data that could be released for an initial analysis.

Creating Scripts

The review team used its initial analysis to review and understand the expense types, attributes, characteristics, relationships, definitions, and unique data properties, giving it comfort with the entire data population and ensuring any results extracted from the total data set reflected the true nature of the data. This analysis enabled the team to organize the data for visualization.

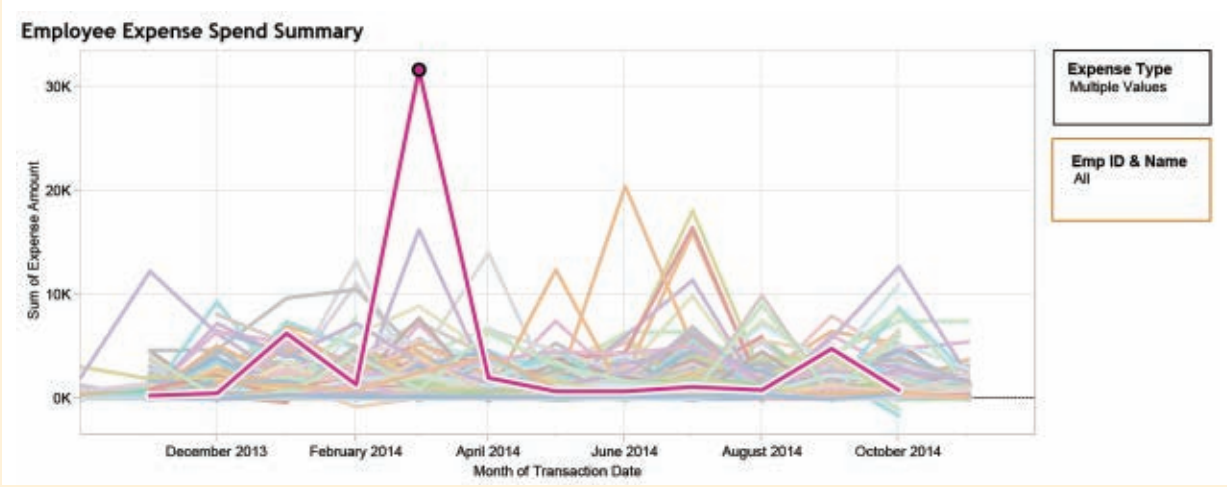
Because the review team lacked experience using the data visualization tool, it contracted with a consulting firm for guidance and assistance in coding the visualization scripts. The team and consultants collaborated to prepare the scripts, define the data attributes, and determine which flags to set as conditions to search and identify transactions.

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

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

EMPLOYEE EXPENSE VISUALIZATION

One of the most powerful data visualization applications is tracking employee expense claims. Internal auditors can dive deeper into data by clicking on the high point in the chart to reveal detailed information about the data point, including employee ID, name, transaction date, and the sum of the total expense.



The consulting firm took the review team's objectives and developed a set of scripts to capture certain data attributes and characteristics for presentation purposes. For example, the review team determined which transaction types represented risks that were higher than average. Other attributes the review team wanted to analyze included unusual transaction amounts, expenses submitted by terminated employees, and duplicate expenses, especially multiple transactions made on the same day, for the same amount, and to the same vendor. The team also used the tool to identify unusual high-dollar or volume transactions made by job classification. For example, comparing a buyer who travels frequently to a salesperson who stays in one location would reveal drastically different spending patterns.

Visual Analysis

Using the visualization tool scripts, the review team generated different reports and data representations. Easy-to-use dialog boxes enabled staff members to request reports to interrogate the underlying data. One of the most valuable reports they generated showed the highest expense spending by a single individual in a chart form (see "Employee Expense Visualization" on this page).

As part of the consulting firm's deliverable, it provided documentation and trained the review team to take over scripting the data visualization tool. The team became more comfortable with collecting, normalizing, and analyzing the data, as well as with building and running the data visualization and then turning over a read-only version for users to run "what if" scenarios and identify suspect transactions.

Generating Solid Evidence

Data visualization can enable auditors to provide management with reports that illustrate suspicious transactions in real time. Instead of sifting through information manually or based on one characteristic, auditors can use data visualization to identify anomalies visually by looking for outliers from expected results and focusing on transactions that have multiple flagged characteristics. Displaying all the underlying transactions that make up a suspicious transaction gives internal auditors solid evidence to support the finding.

The Fortune 500 company's CAE notes that implementing data visualization and predictive analysis should be internal audit's ambition. In today's world, mining data to establish "what happened" is interesting, but answering the question "why?" and being able to venture "what's next" is more valuable. ia

STEVE MAR, CFSA, CISA, *is the IT audit director for a U.S. specialty retailer.*
MICHELLE KHA, CISA, *and* **TRICIA HARDIE,** *audit principals, contributed to this article.*

Risk Watch

BY PAUL SOBEL

WHAT MUST GO RIGHT?

Internal auditors should pay as much attention to the upside of risk as they do to the downside.

Most internal auditors have some experience identifying and assessing risks. They are taught to ask questions of management or themselves, such as "What can go wrong?" and "What keeps you up at night?" These are good questions to ask, but they do not get to the full spectrum of risks that affect an organization. As stakeholder expectations continue to rise, auditors who want to be seen as a strategic asset must start thinking like management and recognize that not all aspects of risk relate to negative events and outcomes.

ISO 31000: 2009, Risk Management—Principles and Guidelines defines *risk* simply as the "effect of uncertainty on objectives." *Enterprise Risk Management: Achieving and Sustaining Success*, published by The IIA Research Foundation, expands on that definition by stating that risk is "the aggregate effect of uncertain events and outcomes on the achievement of objectives." That means that an organization's objectives are affected by uncertain events (which may be good or bad), with uncertain outcomes (which may be desirable or undesirable), causing uncertain effects on the objectives (which may be favorable or unfavorable).

Therefore, when thinking about risk, one needs to understand that risk can have both positive and negative effects. Positive and negative effects represent opposite sides of the same coin. Internal auditors should not limit themselves to focusing on only the negative side of the coin.

Internal Audit's Mission

Each internal audit function has its own charter, and many functions have articulated a unique mission, as well. The International Professional Practices Framework (IPPF) currently is undergoing revisions, which will be released later this year. One key element of the updated IPPF will be the addition of a mission for internal auditing. While the wording of that mission has yet to be finalized, it is expected to emphasize that internal auditing should enhance and protect organizational value.

Protecting organizational value is consistent with most current assurance activities; that is, organizational value is protected when internal audit provides assurance that risks are managed to an acceptable level, controls are operating effectively, and the organization is complying with laws and regulations. Although this type of assurance will continue to be valuable, it focuses primarily on the negative consequences of risk.

However, as the mission implies, internal audit can do more than just

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

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

provide assurance related to the downside of risk. The "enhance" part of the new IPPF mission indicates that internal auditors are in a position to provide assurance and advice that support the long-term value-creation process. This doesn't mean internal auditors are making management decisions, such as approving the launch of a new product, changing product pricing, or expanding into new markets. Rather, internal audit can enhance organizational value by helping management feel confident in taking on more risk. This gets to the upside of risk embodied in ISO 3100's definition of risk.

By helping management embrace the upside of risk, organizational success can be accelerated.

Taking on More Risk

In addition to asking the question, "What can go wrong that can stop us from achieving our objectives?" it's important to ask, "What needs to go right to help us achieve our objectives?" There are many different ways internal auditors can support the key strategic decisions made by management. For example, assurance and advice can help give management confidence that:

- Processes can be expanded or modified to support the production of a new product.
- Market information is current and accurate to support pricing decisions.
- Understanding of anti-corruption and sovereign risks is sufficient, and compliance training and awareness are adequate to support market expansion into a new country.
- The upside and downside risks related to a potential acquisition are appropriately understood and considered in the go/no-go decision.
- Consumer data is adequate to identify shifting consumer patterns, thus supporting key marketing decisions.
- Digital marketing capabilities are sufficient to expand ways in which the organization reaches out to existing and new customers.
- Reports relied on to drive major plant outage and maintenance decisions are accurate, relevant, and timely.

The shift in risk mind-set to expand risk assessment and audit planning to include both upside and downside risks creates many new opportunities for internal audit projects, but also makes the project-prioritization process more complex. Instead of just focusing on projects designed to evaluate whether residual risk is reduced to an acceptable level, other value considerations must be examined, such as whether a project can increase earnings, enhance cash flow, improve the organization's brand or reputation, enhance customer relations, and support the strategic direction of the organization or a particular business segment.

Granted, it is difficult to measure the potential value created—it's more art than science. But the same can be said about measuring the residual risk remaining after the organization has applied controls or other risk mitigation activities.

When deciding which projects to execute, internal audit leaders must consider the "value bet" for each project. This bet should consider the possible ways the project can help protect existing value as well as enhance or enable future value creation. Striking the right balance between the two requires discussion and agreement with the audit committee and management. But a good approach to making value bets, and then assessing the value derived after the project is completed, should satisfy the needs and expectations of both the audit committee and management.

Accelerating Organizational Success

The famous race car driver Mario Andretti once remarked that brakes aren't for slowing you down, but rather are for allowing you to go faster. That sentiment applies to internal auditing, as well. Assurance and advice designed to focus on mitigating the downside of risk is still important, but that only tells management it can tap the breaks when needed. By also helping management embrace the upside of risk, and understanding where it can go faster—and how much faster—organizational success can be accelerated.

Striking a healthy balance in the audit plan between upside and downside risks will help internal audit activities be seen as strategically important to the organization. As a key part of the organization's pit crew, internal audit can help management know when to drive cautiously and when to make a bold move and go for the lead. Internal audit can contribute to effective management of both the downside and upside of risk, asking both "What can go wrong?" as well as "What must go right?" IA

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

26th Annual ACFE GLOBAL FRAUD CONFERENCE

MORE INSIGHT. MORE IMPACT.

BALTIMORE

JUNE 14-19, 2015 / INNER HARBOR

Be more in Baltimore

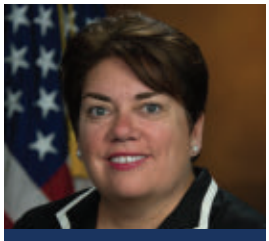
Whether you're adding anti-fraud skills to your résumé or learning advanced investigation techniques, you'll find the resources you need to become a more effective fraud fighter at the *26th Annual ACFE Global Fraud Conference*. Join more than 3,000 anti-fraud professionals from around the world in Baltimore, June 14-19, and experience for yourself why this is the can't-miss event for anti-fraud professionals.

"There is no better anti-fraud training than the annual ACFE conference."

— Rick Panske, CFE, CPA, CFF
Oshkosh Corporation

Keynote Speakers Include:

Brian Krebs
Investigative Journalist, Krebs on Security



Leslie R. Caldwell
Assistant Attorney General Criminal Division, U.S. Department of Justice

James T. Reese
Author, Former FBI Criminal Profiler

Lesley Stahl
Co-Editor of "60 Minutes"

more insight

more connections

more impact

Register by March 25 to **save $200!**
FraudConference.com

ACFE
Association of Certified Fraud Examiners

Fraud Findings

BY ALISTAIR BEAUPRIE EDITED BY JOHN HALL

THE "FAKE PRESIDENT" FRAUD

A fraudster dupes an unsuspecting employee by impersonating a company executive.

"This is urgent," "this needs to remain confidential," and "I'm relying on you." These were the phrases that the man on the other end of the phone repeated to Catherine Martin, an accounts payable clerk in the Belgian branch of Evergreen Inc., a Toronto-based company. Once she hung up, she corresponded with the man via their personal email accounts, per his instructions.

Martin believed she was speaking with Fraser Durand, the chief financial officer (CFO) of their medium-sized manufacturing company, and that she was helping to resolve payment to a subcontractor because Evergreen's usual account was in overdraft. In truth, Durand had no knowledge of this transaction and had not spoken to anyone in the Belgium division in more than a week. "Durand" was actually the perpetrator of an increasingly common deception known as the "fake president" fraud.

The perpetrator emailed Martin an invoice for €612,000 (US$694,000) from a Moldovan company with details of a bank account in Moldova. Martin had not heard of Evergreen doing any business in Moldova, but as the orders came directly from "Durand," she was not as suspicious as she might have ordinarily been. The email was flagged as important, and, while the message had grammatical and spelling mistakes, it clearly explained that the money was to be transferred immediately and payment was to be divided into increments of approximately €15,000 (US$17,000).

For the next few hours, Martin received several other calls from "Durand" inquiring about the transfer. Payment was delayed because Martin needed the approval of Michel Lemaire, her supervisor in Brussels. Lemaire was out of the office, so Martin contacted him on his mobile phone, indicating the amount and purpose of the transfers, and urged him to act quickly. Lemaire accessed the company's banking website from home and approved the transfers without asking for supporting documentation.

The following morning in Toronto, Liz Bertrand, Evergreen's controller, logged onto the company's banking website as she did every morning before the start of the workday. Between sips of coffee, she noticed a series of transfers to an account in Moldova. As these transfers had been initiated and approved in Brussels, she called Martin. Martin told Bertrand that the transfers had been done at the request of Durand and provided the invoice. Bertrand then spoke to Durand, and they quickly realized the company had been the victim of a fraud.

Bertrand and Martin scrambled to call their bank and halt or recall the transfers, but it was too late: Transfers totaling €186,000

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

IIA
Audit Group Membership

Join. Save. Succeed.

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

"My entire team stays on top of industry issues with IIA's timely updates and position papers. We're invited to complimentary educational programs that we can easily fit in our schedules because they're offered as webinars and podcasts or in person."

Nicole Degnan

Chief Audit Executive
The Blackstone Group
New York, New York

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

The Institute of Internal Auditors

2015-5010

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

(US$211,000) had been successfully sent to Moldova. The Belgium office filed a police report and began to prepare an insurance claim. Ultimately, the perpetrator was able to successfully withdraw the proceeds of the fraud and escape justice.

This fraud was successful for a variety of reasons. First, the perpetrator had done his homework by researching Evergreen thoroughly. Information about Evergreen executives was publicly displayed on the organization's website, and company promotional videos may have helped the perpetrator to perfect Durand's accent and mannerisms. Knowing details such as reporting lines, names, and titles of employees helps perpetrators avoid arousing suspicion. This practice is known as social engineering, and it is an increasingly powerful tool available to perpetrators in the digital era.

Social engineering is an increasingly powerful tool available to perpetrators.

The second factor behind the perpetrator's success was his knowledge of corporate policy. He had an invoice on hand to justify the payment to a "subcontractor," adding legitimacy to the transaction, and asked for the payment to be split into increments—a practice known as *structuring*. By splitting the amounts into smaller increments, the perpetrator was able to avoid the usual authorization limits and approval process around cash disbursement. A perpetrator may not know the exact authorization limits, but may specifically ask the target or simply guess at common limits for an employee based on his or her title. Perpetrators also have been known to assume the identity of a genuine supplier or vendor, while providing the targeted employee with new, fraudulent banking details and asking him or her to pay all unpaid invoices. Additionally, some perpetrators will add legitimacy to their email communication by copying an unwitting external professional in email communications—perhaps a partner in a law or accounting firm.

The biggest advantage that perpetrators of this fraud have is that it is easily repeatable with other companies. If discovered, a perpetrator will likely just hang up and move on to the next target. Perpetrators typically use a prepaid, disposable mobile phone and operate out of jurisdictions with lax enforcement, minimizing the chance of being caught. As the dollar values involved in these schemes are high, perpetrators only need to be successful once to make it worth their while.

In this situation, the targeted employee did not notice, or failed to act upon, several red flags. The use of bogus personal email accounts designed to spoof the details of the person the perpetrator is attempting to impersonate such as "Fraser@gmail.com" is common. Alternatively, perpetrators may use email accounts designed to approximate genuine corporate email accounts such as "CFO@compaany.com" (often with extra vowels or other small misspellings). Spelling and grammatical mistakes are another red flag. Company or banking details in countries that are known to be at risk for fraud or not known to be areas where the company does business are also indicators that the transaction may not be genuine. Finally, a sense of urgency from the caller and a desire for confidentiality and to circumvent controls are common in such schemes.

Lessons Learned

- Employees should be educated about the "fake president" fraud and similar schemes. Internal auditors can help by offering formal training that ensures employees are aware of the red flags and are encouraged to be skeptical. Upper management should visibly buy into these efforts by publicly stating their approval, and show potentially targeted employees that it is acceptable to challenge suspicious requests for payment.
- Internal auditors can perform an internal controls review of the cash disbursement function in light of the "fake president" fraud. Payments should not be made to an organization or bank account not already in the vendor master file. Changes or additions should always be approved by more than one employee and confirmed with a known contact at the payee. Controls on approval limits should be adjusted to prevent the structuring of payments or transactions to pass beneath limits.
- Every company should have a financial authority limits policy that provides employees clear direction with respect to the approval process. Internal auditors can perform a review to ensure that the policy is followed.
- Employers should be aware of the information employees make public via social networking websites—especially LinkedIn. Formal training offered by the internal audit department should cover the risks posed by social media.
- Internal auditors should consider reviewing information the firm makes public on its website, such as employee positions, email addresses, and phone numbers. IA

Alistair Beauprie, CPA, CA, CFE, *is a senior accountant at EY in Montreal.*

Arthur Piper

Audit departments of limited size can learn a lot from their larger counterparts, but they have much to teach as well.

When Denis Bergevin stepped into the role of deputy director in charge of the Internal Audit Division at Caribbean Development Bank, Barbados, in May 2014, he knew it would be a challenge. The bank had already upgraded its risk management function and some of its compliance activities. Now it wanted to achieve the same with internal audit—a move fully supported by the organization's senior management.

"They had never had an experienced internal auditor at the helm of the department before," he says. "They did have a very solid charter, so that was my starting point—to sit down with them and explain to them what internal audit should do."

But with a team of just four people—including Bergevin—resources and time are tight. Not only that, but for the past 40 years internal audit at the bank has focused largely on compliance. One of his first moves was to ensure that other compliance functions and management took on that role to free up his team.

Communicating these changes to management has been key, says Bergevin, who has allocated two or three days a month to this task. In addition, he has devoted about three of the past eight months to developing a list of relevant audits as well as the criteria he will use for audit selection. With limited resources, it is crucial to get the focus, depth, and duration of each audit right, he says.

Modernizing a small function in this way depends on taking the best practices larger audit functions use and making them work in an alien environment—where people and time are extremely limited. For Bergevin, working at the bank is a world away from previous roles—including more than seven years spent in Audit and Risk Management Services at the Canadian telecom giant Bell, which at one time boasted a team of 135 internal auditors. But he is optimistic that the practices he learned at

Small Audit Functions Big Ideas

Bell and elsewhere can be used to transform his department.

Bergevin also says that the way small audit functions operate can provide useful lessons for larger functions. He says smaller departments eliminate the narrow skill specialization of staff in larger departments because every person on his team has to be capable of taking on most audits. Auditors also have closer contact with senior management, something that seldom occurs in a larger function. And, he says, auditors in smaller teams develop better business acumen because they are close to the action.

"In a small audit function, the internal auditor who did the work is the one presenting the findings to the highest level of the organization," he says. "That helps the auditor build relationships and understand how management thinks."

Even if small audit functions often face larger hurdles, the truth is that functions on both ends of the size spectrum have a lot to learn from each other. Differences in the way small departments are funded and trained, and how they operate, offer fertile suggestions for improvement for large functions, and vice versa.

"In a small audit function, the internal auditor who did the work is the one presenting the findings to the highest level of the organization."

Denis Bergevin

CUTTING THE WASTE

Because resources are constrained in small audit functions, they have to be accurately and parsimoniously employed so that waste is reduced to a minimum. That does not always happen, of course. Many small functions do not have the leadership, experience, and skills to implement such initiatives. Many are stuck in a compliance rut. And many small function audit executives are low down the business' leadership hierarchy, without authority to make the sort of sweeping, strategic changes that Bergevin is introducing.

But that does not mean they cannot adopt big function best practices if they remain focused and selective. James Paterson has used his experience at large audit functions — including a stint as vice president of Internal Audit at the global pharmaceutical company AstraZeneca — to develop a "lean approach" to internal auditing, which he says could help small functions concentrate on the fundamentals of best practice.

"A mistake that smaller audit functions can make is to hunker down, lose sight of the broader picture, and focus only on one major audit."

Charles Windeknecht

Now a director of the consultancy Risk and Assurance Insights in Manchester, U.K., and author of the book *Lean Auditing: Driving Added Value and Efficiency in Internal Audit,* Paterson says he believes in focusing rigorously on driving value and productivity. Key to that strategy is developing close relationships with senior management and the function's other stakeholders to ensure that the work performed has real value to them. In many ways, that is something small audit functions are as equally well-placed to achieve as their larger counterparts, he says, because the head of audit is often the one performing the work and talking directly to the clients.

"Small audit functions need to be the most plugged in to management and smart at making choices about what to do," he says. "That's key because when they devote resources to something, it is always going to be a significant proportion of their budget, so effort has to be directed at the right thing."

As well as ensuring that any other compliance and assurance functions are producing quality work, he says the function's job is to drive accountability for management and fix its problems. For example, he sees little point in auditing a known issue unless management has already started work on fixing it and the value from any audit work is clear. For example, audit's value might come from helping to identify the root cause of a problem, or to review the progress management has made in fixing it.

In addition, Paterson says assignment planning should, in most instances, be approached like a mini-project, with clear deadlines and a sense of the value that will be created. That can often entail

prioritizing the scope of the work and being clear about what a helpful result might be. "This approach tries to avoid coming up with audit findings that are simply housekeeping points, or within management's risk appetite," he says.

He adds that lean auditing can encourage greater flexibility in assignment types. "A small audit function may be much more likely to generate value from, say, two 25-day assignments than from one 50-day assignment," he says. "If stakeholders want more on the issue after a 20- or 25-day assignment, you can then identify another specific area to look at next, rather than just using up 50 days in a scattergun way."

He admits that lean auditing requires much more planning and information gathering at the beginning of the process to identify the right areas of focus and the key areas where value can be added. The upsides are that the audit will often progress in a more purposeful way and, when audit work is produced, it has a far greater chance of being valued by the client.

TAKING TIME WITH STANDARDS

To small audit functions, compliance with The IIA's *International Standards for the Professional Practice of Internal Auditing* (*Standards*) may be seen as prohibitively time-consuming. "The main challenge that small functions face on the *Standards* is finding the time to take account of the different constituencies you serve in the organization and determine where your focus needs to be," says Charles Windeknecht, vice president of Internal Audit at the global airfreight business Atlas Air Worldwide in Purchase, N.Y.

Bypassing this step is a false economy. When he took over the reins at Atlas Air more than seven years ago, his first priority was to carry out a current state assessment against the *Standards* to see how well internal audit was performing.

"I shared the initial results with the chief financial officer," he recalls. "The assessment gave us a framework, some definable standards to work to, and a roadmap for us to improve in specific areas where we knew we could do better." He also says that it gave him an opportunity to educate senior management about the *Standards* and provide transparency and honesty about the function's current performance. Without taking the time to go through the process, the function would have lacked direction and been less engaged with senior management.

The 2015 head count for Atlas Air's internal audit department is eight full-time posts. So, Windeknecht knows from experience that performing a self-assessment can be tough while trying to keep the function working. He says heads of audit at small functions can manage it by staying practical and organized, and by keeping the process as simple as possible.

LOOKING FOR CAPACITY

Windeknecht says one major challenge of running a small audit function is ensuring a high degree of collaboration among team members and with the business owners. The challenge is more daunting with smaller teams, as there is often only one person conducting each audit. "A mistake that smaller functions can make is to hunker down, lose sight of the broader picture, and focus only on one major audit," he says. "But IIA members have set up some great networks to plug into and share knowledge and information in an informal and collaborative way, which can save a lot of time." He says that he has benefited numerous times from his participation in the Airlines 4 America internal audit networking group, for example, and local IIA chapters.

Windeknecht says small firms often have a surprising amount to offer their larger counterparts in terms of sharing information in these networks. He

A MATTER OF SIZE

Most internal auditors work in small audit functions. In its State of Internal Audit Survey 2012, Thomson Reuters estimated that 67 percent of functions have fewer than 10 people working in them and 80 percent have fewer than 20. But defining what constitutes a small audit function can be tricky, according to David O'Regan, author of *Strategies for Small Audit Shops*, now in its second edition.

"Whether one approaches this matter in either absolute or relative terms, it tends to be difficult to avoid a certain amount of ambiguity," he says. "In absolute terms, an audit department that consists of one to three auditors is certainly small in most circumstances, yet a 30-strong team might also be considered small in some contexts."

He says there are comparative metrics that can be useful in determining how small a function is in relation to its peers—for example, the ratio of the number of auditors to revenues or assets and the size of the audit budget as a percentage of the organization's total budget. "In the end, I think a definition is dependent on organizational and sector context, and it should take into account the head count, the levels of experience of individual auditors, and the amount of budgetary resources at the disposal of the audit department," he says.

recently shared his function's entire quality assurance program with a department five times larger than his own, and he has also passed on advice about how to update an audit charter to another large function. "You can't be shy to reach out to the big functions and the forums," he says, "because you will find the way you work is likely to be of interest to them—it cuts both ways."

One advantage small functions have over their large counterparts is their ability to be closer to management and understand their needs thoroughly, which can make their processes practical and relevant to the industry they serve. "Large audit functions don't always get the pulse of their organization from the perspective of its entrepreneurial spirit, or from a strategic growth standpoint," says Alyssa Martin, advisory partner at the independent accounting firm Weaver in Dallas. "Large functions become a little bit more isolated from the nerve center of the organization."

She says this knowledge can make smaller audit functions more nimble and responsive to management plans and better able to keep close to the business' strategy. In addition, small audit teams, when working well, tend to focus more on making the business better, rather than on compliance—a lesson large functions could do well to learn, she says.

Yet even the most plugged-in, highly focused small audit function can suffer from lack of capacity, something that is made worse because of the limited range of staff that work in such functions. "Every small function is at the mercy of the background and expertise of the individuals on the team," Martin says. She says a team of three to five auditors is unlikely to have the in-house expertise to cover every financial, operational, strategic, and IT issue in depth. And while hiring staff to deal with IT risk, for example, is a problem for the entire profession, the

"Large audit functions don't always get the pulse of the organization from the perspective of its entrepreneurial spirit."

Alyssa Martin

"Go for one process, one tool, even just a few features within that tool, so you fully master what you are implementing."

Mike Gowell

SEE "Eye on Business," page 66, for more on small audit functions.

budget needed to buy such expertise for a small function could be prohibitive.

Martin says audit functions can work with their peers in noncompetitive industries to plug some of that gap—a practice common in larger organizations. In the retail and banking sector, for example, she knows of CAEs who peer review noncompeting businesses in quality assessment exercises. It is a form of skills bartering and exchange.

"Of course, you have to be sure that from a strategic and intellectual property perspective those peers are truly noncompetitive," she says, "but it can be a much better option than buying that expertise on the high street."

As a provider of cosourced internal audit services, Martin supports the idea of hiring skills where they are needed—a strategy followed by audit functions of all sizes. But she warns that on a per-hour basis, cosourced hours are always likely to be more expensive than those spent by in-house staff.

Recruiting in-house presents challenges as well, and Martin urges heads of small functions to balance their needs realistically: "I think you have some that you know are going to be highly ambitious and critical thinking and you might be able to keep them, from a retention standpoint, for a year or two," she says. "You have others who you want to keep long-term, and they perform consistently and have good auditing skills."

MAKING THE MOST OF IT

While large audit functions have bigger budgets for hiring staff, they also have more money to spend on audit software tools and IT training. That means staff in small functions are most likely to be trained on IT tools in-house, but that has had some surprising results.

When the technology services company Wolters Kluwer Audit Risk and Compliance conducted a survey of nearly 300 small function internal auditors—Audit Technology Insights 2013—it found that small functions were 20 percent less likely to be using data analytic tools, and only 35 percent of small functions said that their IT budgets would increase (compared to 42 percent overall). Smaller departments were using cheaper solutions—such as Excel and Access—for data analysis. But 28 percent of small audit function respondents said all staff members on their teams were "fully proficient" with their audit technology tools, compared with only 18 percent of large-function respondents.

"We were surprised by the degree of technology use by the small functions," says Mike Gowell, general manager and vice president of TeamMate, an operating unit of Wolters. "Those who can afford the technology and acquire it want to wring a lot out of it."

He says small audit functions need to take an incremental approach to their IT acquisition and training. "Go for one process, one tool, even just a few features within that tool, so you fully master what you are implementing," he says. This helps selling the benefits of IT spending to senior management, who can see incremental improvements to the efficiency of audit work, he adds.

SHARING KNOWLEDGE

It would probably surprise some that with their limited resources, small functions can teach their larger counterparts lessons—but the very existence of those constraints have lead to efficient practices that bigger departments would do well to emulate. Similarly, larger functions' broader range of industry knowledge and up-to-date best practices can be of great benefit to small function heads of audit and their staff. Sharing such experiences and knowledge should be a priority for both groups of auditors. IA

Arthur Piper *is a writer who specializes in corporate governance, internal audit, risk management, and technology.*

Imagine What You'll GAIN Turning Your Information Into Insights.

Do you want to know how your internal audit department measures up? The Global Audit Information Network® (GAIN®) Benchmarking Tool allows you to benchmark your internal audit department easily, affordably, and transparently. It lets you compare your audit department's size, experience, and other metrics against the averages of similar organizations in peer groups that YOU choose.

Find out how you compare with your peers with reliable data and metrics including:

- Performance measures.
- Organizational statistics.
- Department staffing and costs.
- Operational measures including audit life cycles.
- Risk assessment and audit planning information.
- Oversight including audit committee information.

No matter what your benchmarking needs are, the GAIN Benchmarking Tool has you covered. Your final report will benchmark your organization with participants in 17 industries, more than 100 sub-industries, and 42 countries, unlocking real answers to organizational questions.

Get Started Today!
Visit www.theiia.org/goto/GAIN

The Institute of Internal Auditors

2015-5022

Digital Signatures Deciphered

Shiva Hullavarad
Russell O'Hare
Ashok Roy

Internal auditors should assess the business processes and risks associated with signing documents digitally.

In today's digital business environment, internal auditors have to assess the risk and security of large volumes of digitally originated transactions and documents. Among the many methods, protocols, and products for securing online transactions are digital signatures. For example, the mortgage industry uses digital signatures for approving real estate negotiations by affixing them to price or contract changes until both parties agree on terms and a price. Once they have reached an agreement, the parties execute the title transfers with a notarized ink signature.

Digital signatures improve efficiency, provide security around transactions, and enhance collective approvals in a fraction of the time compared to conventional ink signatures. Nonetheless, there is always the danger and fear of unauthorized or malicious use of digital signatures. Internal auditors and organizations need to assess the level of risk and to what extent the organization should secure its digital

signature platform. Moreover, auditors should consider the trade-off between the level of risk digital signatures pose and the level of authentication required to provide desired levels of assurance while accepting them.

PROOF OF AUTHENTICITY

A digital signature is an electronic sound, symbol, or process attached to or logically associated with a record and executed by a person with the intent to sign the record. In layman's terms, it is a person's electronic expression of agreement to the terms of a particular document with the intent to sign. A scanned or photographed image of a written signature does not constitute a digital signature, as it is analogous to affixing a rubber stamp of the signature that can be duplicated or misused without the signer's knowledge. Instead, digital signatures provide a secure encryption environment for the data associated with a signed document and verify the authenticity of a signed record.

To authorize transactions, digital signatures use a combination of content capture, method of signing, data, and user authentication. They use electronic authentication to establish confidence in user identities that are electronically presented to an information system. Individual authentication is the process of establishing an accepted level of confidence and assurance for an accepted level of risk.

There is a direct relationship between the associated risk and the complexity of authentication needed to provide a higher degree of assurance in the use of digital signatures. Higher levels of assurance need complex, multifactor authentication methods that, in turn, require a secure IT infrastructure and user training. This correlation poses a trade-off challenge to auditors and organizations willing to accept digital signatures, thereby compelling them to identify those business processes that require an optimum level of authentication to offset risks.

Digital signatures are built on an encryption/decryption technology that a) collects evidence of the document such as metadata and IP address, b) verifies the identity of a signer and receiver, and c) provides an audit trail of the transactions. This technology uses a public key infrastructure (PKI)

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

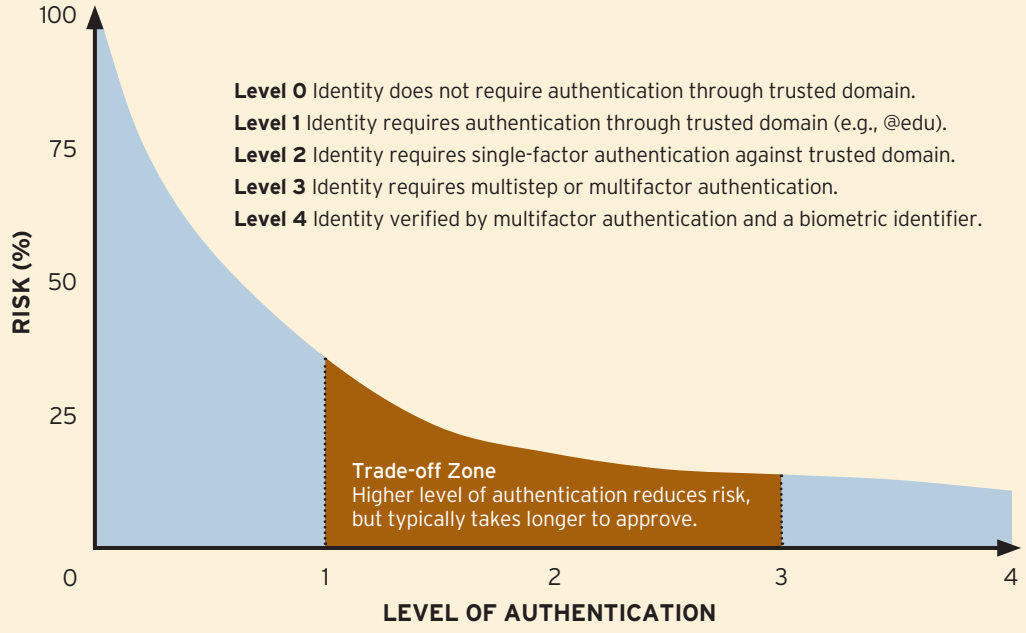
HOW DIGITAL SIGNATURES WORK

Digital signatures use private/public keys and hash results of the original and destination documents. The digital representation or summary of the document unique to a message *origin-hash result* (OHR) is created by the hash function of the digital signature software. In turn, this software uses the signer's *private key* to transform the hash result into a digital signature that is unique to the message. Upon receipt of the document, the transmitted message computes a new *destination-hash result* (DHR) by using the same hash function used to create the digital signature. Using the corresponding *public key* and DHR, the receiving computer confirms whether the affixed digital signature was created using the matching private key and whether both the OHR and DHR match. If both the keys and hash results are a match and confirmed, the validity of the message, signer, and receiver are verified.

81% of digital signature projects achieved return on investment within one year, according to the 2013 Digital Signatures survey by the Association for Information and Image Management.

DIGITAL SIGNATURE RISK TO AUTHENTICATION

The chart below illustrates the digital signature risk-to-authentication model. This model provides a semi-quantitative approach to assess the associated risk for a given level of authentication used to provide a digital signature.



in which the signer uses his or her private key to encrypt the document and the recipient uses the corresponding public key to decrypt it (see "How Digital Signatures Work" on page 36). A digital signature requires a signer to establish a certificate-based digital ID, commonly enclosed in a token, smart card, or other physical device, to provide a high level of authentication, integrity, and security to the transaction and the identity of the parties signing. The executor or signer is presumed to be legally responsible for any document signed with a private key.

The important consideration when assessing the risk for digital signatures is their provisioning through e-mail communications, which makes Internet security critical. If the e-mail platform is compromised, the digital signature and PKI lose their authenticity and validity.

THE RISK–ASSURANCE TRADE-OFF

"Digital Signature Risk to Authentication" on this page depicts the trajectory for risk tolerance versus level of authentication for a typical business process. The trajectory slope may vary with the nature of the business process. For example, financial transactions, approvals, or decisions generally have a higher degree of risk, based on their monetary value, than administrative functions such as leave requests.

The digital signature risk-to-authentication (SRA) model depicted in the chart provides a framework for internal auditors to establish the desired level of trust for an electronic transaction, as well as the authenticity, integrity, and reliability of such transactions. This can be accomplished through a quantitative risk assessment for each transaction specific to a functional unit by estimating the risk and the likelihood of occurrence. Use of the SRA model can give internal auditors an understanding of internal controls and security needed when their organization implements digital signatures.

The SRA model provides a semi-quantitative approach to assessing the risk associated with a given level of authentication used to provide a digital signature. As a general rule, the higher the level of authentication, the lower the likelihood that an incident, or breach, will occur and the

AUTHENTICATION LEVELS

Authentication focuses on confirming the authenticity of the document and the validity of the signer based on pre-established and verified credentials. This table shows the authentication levels, equivalent electronic modes of authentication, and risk of compromise.

Level	Signer's Identity Verification Description	Electronic method	Risk of compromise
0	Unknown	Unknown domain email, suspicious email domains.	High
1	Requires validation with IT	Organization employee directory generated user ID and password or organization email.	Medium
2	Level 1 + single factor	Organization email + digital signature (PKI).	Low
3	Level 2 + double factor	Organization email + digital signature + workflow.	Lower
4	Level 3 + biometric	Organization email + digital signature + workflow + approver.	Lowest

lower the risk. Although the nature of the risk versus authentication curve may be different for different business processes, the pattern will tend to follow the path of reduced risks for higher authentication. Internal auditors or management can develop a risk chart based on the formula: *Risk (R) = Likelihood of occurrence of event (L) x Magnitude (M).*

To illustrate the formula, assume that one in 30 email accounts are hacked. Based on this assumption, the risk can be calculated by assessing the monetary magnitude of the effect of hacked emails on an organization. The trade-off zone depicted in the chart provides an opportunity window to secure the digital signature environment to achieve the desired level of assurance, thereby enabling organizations to identify those processes that require optimum levels of authentication to offset risks.

The key factor to consider in implementing digital signatures is to identify the level of risk tolerance and the associated risk for a business process. Institutional risks may involve financial, brand-value reputation, and other key administrative communication. Based on the various types of business processes and the level of severity, the assurance levels — which are a combination of authentication and validation — as well as the trust levels must be established by the appropriate business-unit management. To secure an electronically signed document as evidence, auditors should consider the risks associated with the signing process and with the significance of the information. Security must be approached with the objective of managing potential risks and should be weighed against the level of authentication needed to achieve the desired level of risk tolerance (see "Authentication Levels" on this page).

Internal auditors can use this model to assess the risk/assurance needed for digital signatures. Because systems are imperfect, auditors should consider the reliability of the information obtained through the digital signature validation process. For example, they should consider whether digital signatures can enhance internal control over online sales orders by authenticating the validity of customers.

DIGITAL ASSURANCE

As the Internet is an essential tool for transmitting digital signatures, it is necessary to have a secure transmission process that ensures a document signed through a digital signature is not tampered with by a third person and reaches the recipient in the form in which it left the signatory. Organizations also need to determine which business processes are not appropriate for digital signatures, such as creating wills, testamentary results, and certain types of contracts.

Internal auditors and their organizations need to identify the various processes for which they plan to use digital signatures, as well as perform a comprehensive risk assessment of those processes. The digital signature risk to authentication model can help auditors assess the level of authentication suggested for a specific business process to ensure it provides the desired level of assurance.

SHIVA HULLAVARAD, PHD, *is statewide ECM/ERM System Administrator with the University of Alaska System in Fairbanks.*
RUSSELL O'HARE, EDD, CRM, *is chief records officer with the University of Alaska System.*
ASHOK ROY, PHD, CIA, CFSA, CBA, *is vice president for finance and administration with the University of Alaska System.*

We Are Proud to Be Internal Auditors!

As internal auditors, we're proud of our profession. So why not celebrate and help the world understand what internal auditing is all about? It's not about accolades. It's about awareness.

May is International Internal Audit Awareness Month, and The IIA is encouraging members, chapters, and institutes around the globe to spread the message of the value internal auditing brings to an organization and the business community.

Download The IIA's updated Building Awareness Toolkit, featuring creative ideas, tips, tools, and templates for promoting the profession in May and throughout the year.

Mark your calendars for International Internal Audit Awareness Month: **May 2015!**

PROUD TO BE AN INTERNAL AUDITOR
INTERNATIONAL INTERNAL AUDIT AWARENESS MONTH–MAY
www.theiia.org

Show the world you're proud to be an internal auditor with the 2015 International Internal Audit Awareness Month celebration icon!

www.theiia.org/goto/awareness

The Institute of Internal Auditors

2015-5024

Russell A. Jackson

Illustration by Doug Ross

A smart approach to U.S. Affordable Care Act compliance begins with a comprehensive risk assessment.

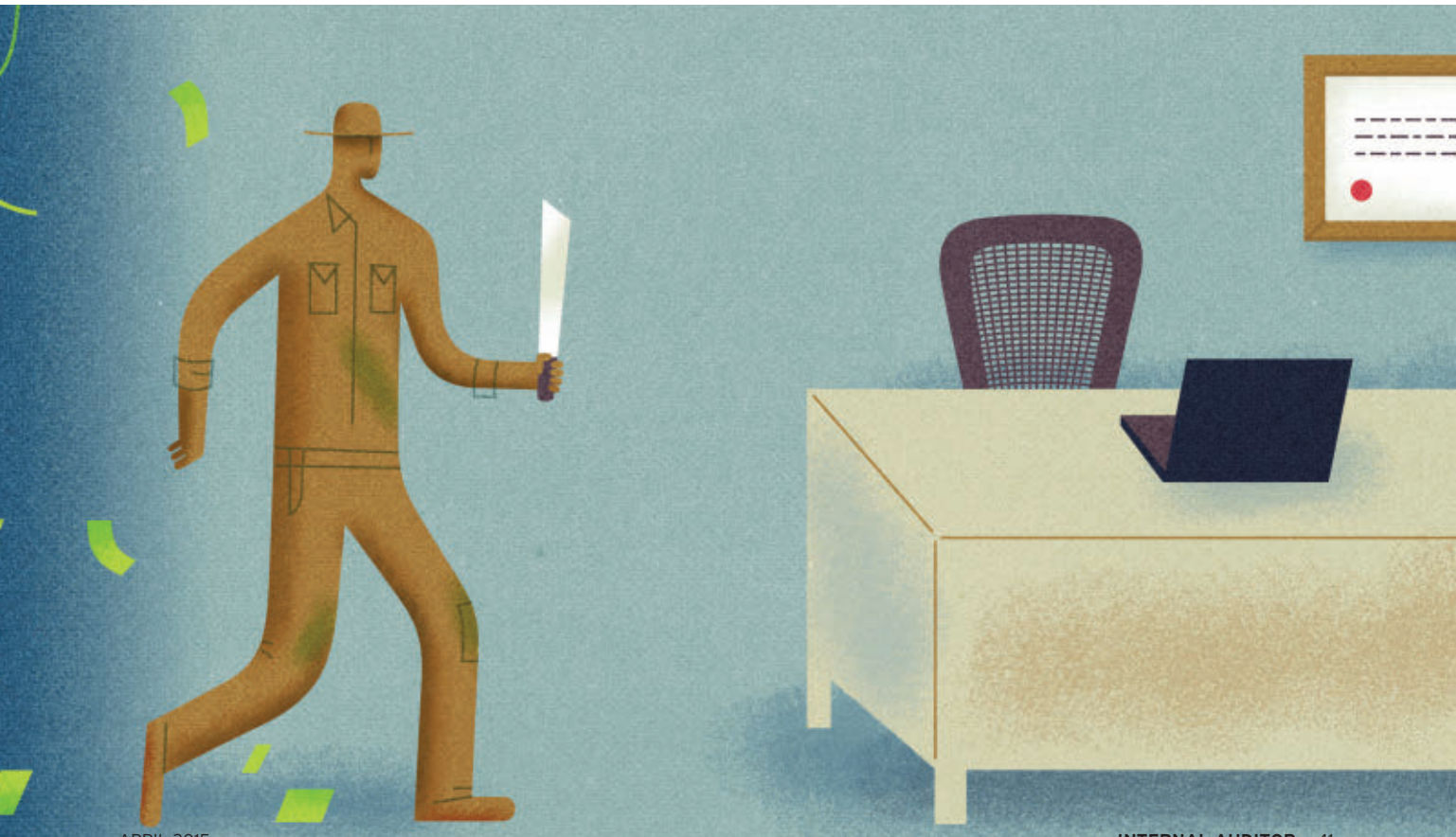
Untangling the ACA

Judging by what's been said about the U.S. Patient Protection and Affordable Care Act (ACA), it's no wonder it's been perceived as too complex for any but the most dedicated Washington, D.C., policy experts to understand. Yes, the ACA is dense. No, compliance won't be easy. And auditing readiness for compliance—and compliance itself—won't be easy, either. But internal auditors who've been through the fire say that once you get an idea of your organization's risk profile in relation to the act, you may be able to sit back for the time being and focus your attention on other risks that pose a bigger threat.

"It's not as scary as you might think," reports Annette Schandl, senior vice president of audit at CHAN Healthcare, based in Clayton, Mo., a subsidiary of Crowe Horwath LLP. "From an internal audit perspective, management should have specialists in place to implement the ACA. Once the implementation is complete, internal audit should perform testing of the process." Internal audit, she adds, needs to have a seat at the table as ACA policies and procedures are developed, to make sure the right controls are considered. But the bottom line is this: Auditing is still auditing, no matter how Byzantine the beast.

That's not to diminish the frustration and confusion organizations are experiencing in the face of something that's received so much scrutiny and been the subject of so much commentary. "It's just too complicated," says Emily Friedman, an independent health policy and ethics analyst based in Chicago. "Even human resources professionals are having problems knowing what to do."

Indeed, a recent report from human resources (HR) and payroll consultant ADP shows that more than half of companies with at least 1,000



employees are unprepared to comply with all of the ACA's regulatory requirements. Key components of the law that pose particular compliance problems, ADP says, include Exchange notices, penalties, and reporting required to the U.S. Internal Revenue Service—all areas that internal audit will likely need to help rank order by risk and then compliance, which they'll need to assess.

Additionally, many larger companies are using benefits strategies that shift more costs to employees in the wake of the excise tax on high-value health plans that becomes effective in 2018; others are limiting hours for some employees to avoid the coverage mandate. Employers now have to count "hours of service," notes Jerry Healy, employee benefits counsel for Keenan & Associates, in Torrance, Calif., calling it "a new defined term not commonly used for benefits." As such, he adds, the term not only has to assimilate into the workforce and its medical plans, but maybe also into collective bargaining agreements. Many firms don't have the systems in place to track and report that new information.

Other items that need to be addressed, he adds, include special transition rules, communications to employees, U.S. Department of Labor audits of certain health plans, and the Mental Health Parity and Addiction Equity Act. Even if those are areas new to internal auditors, the tasks internal auditors need to perform in response are not. Complying with the ACA will be difficult for most firms, but those firms' internal auditors can accomplish their part in it by focusing on performing tasks they are familiar with and not be daunted by the unfamiliarity of the entire act.

RISK ASSESSMENTS

The trickiest part of compliance for Bellevue, Wash.-based Nordstrom was "anything related to the Cadillac tax," notes Dominique Vincenti, vice president, internal audit and financial controls. But she adds that the difficulty was largely self-inflicted, because the company maintains both an HR and benefits department and a tax department, and "some of the taxes that the company had to deal with are managed by the HR department and not the tax department." Each thought the other was taking care of it, so no one was taking care of it.

But a detailed risk assessment—which her department conducted specific to the ACA—turned up the fact that the management team had not thought clearly in terms of roles and responsibilities and the tax implications of the ACA. "We caught it very early," she says now, "which allowed us to highlight to management the intricate complexities of the tax implications and to get both departments at the table to agree on allocation of roles and responsibilities."

She adds that, because of that detailed risk assessment, her team's role in helping the department store chain address the ACA is largely complete—

Even if the ACA presents areas new to internal audit, the tasks auditors need to perform in response are not.

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

The Congressional Budget Office estimates **US$8 billion in penalties** will be collected by the U.S. Internal Revenue Service from employers who misclassify full-time employees.

at least for now. "The ACA, like any other law or other regulation we have to comply with, is part of this big compliance pool made up of a bunch of stuff," she explains. "It's no worse or better than the others. It's one of many." In fact, she states simply: "We feel at this point that the ACA doesn't rise on any radar. It's been very quiet." The company's general counsel maintains compliance oversight responsibility. Vincenti meets with him twice a month to "see if anything is starting to bubble up."

Sharon Gipson, vice president, corporate audit, at Detroit-based Blue Cross Blue Shield of Michigan, agrees that a smart approach to ACA compliance starts with a comprehensive risk assessment. "You need to understand what pieces of the ACA are applicable to you and make some decisions about what to focus on," she says. Essentially, she advises considering not only internal processes, but partners and vendors as well because, she notes, "they can introduce as much compliance risk into your organization as you can within the organization." Then, of course, you "lay out how to address the higher-risk areas first," she says. "Once you have an understanding of which portions of the ACA impact you and how they've been implemented and are operating within your organization, you can focus your efforts."

Consider internal processes as well as partners and vendors.

BUSINESS AS USUAL

If that sounds a lot like what internal auditors do every day, that's because it is. Ensuring employer readiness and compliance, says Gwendolyn Skillern, senior vice president and general auditor at CareFirst BlueCross BlueShield in Owings Mills, Md., involves "processes and types of audits that are familiar to an internal auditor." It requires analysis of complex processes that many internal auditors likely have never faced before. But while "you may not be accustomed to the complexity," she adds, "you do know how to initiate inquiries needed to assess risk. We worked very closely with the business to find the information needed."

She says her company formed a health reform steering committee that divided compliance into five tracks. "We embedded an internal auditor in each one," she says, "so that as the company developed compliance strategies, we understood them and could efficiently direct our audit activity." That's critical, she emphasizes, "as the auditors cannot work in a vacuum. At the end of the day, we are in partnership with the business to mitigate the risk to the company. The ACA is too complex and too fast-moving. You can't work in a silo and then show up to conduct an audit."

Carl Mowery, managing director, compensation and benefits consulting at Grant Thornton LLP in Chicago, agrees that internal auditors won't be mystified at the specific tasks required to audit for ACA readiness and compliance. "Conceptually, it's the same thing," he says. "If an internal audit department is accustomed to doing employee benefit audits, it's similar to those, but a little bit more detailed." In many benefits audits "some leeway can be had," he adds, "but the ACA really

"The ACA, like any other law or other regulation we have to comply with, is part of this big compliance pool ... it's no worse or better than the others."

Dominique Vincenti

"You need to understand what pieces of the ACA are applicable to you and make some decisions about what to focus on."

Sharon Gipson

does not provide much flexibility, so particular attention will have to be paid to the details."

MEETING REQUIREMENTS

Many of the most challenging of those details will arise as internal auditors "really look at the controls processes and procedures that have been implemented to determine who is a full-time employee and track those employees from the perspective of the reporting and record-keeping requirements of the ACA," Mowery adds. "If an organization does not have those controls processes in place when the external auditors come, it may have to record a contingent tax liability."

Generally, there is a US$2,000 penalty per employee for not having offered coverage to 70 percent of full-time workers; that percentage rises to 95 percent next year. "Part of the compliance process is understanding who is a full-time employee and who is not," Mowery notes. "Be sure to look at independent contractors as well as leased employees." Under the ACA, the common law standard is used to define who is an employee; a full-time employee works on average 30 or more hours a week.

Some suggestions about what internal audit departments can do now to make sure those and other requirements are met include:

Make sure you have a seat at the planning table. "As the ACA is being rolled out, we follow several months behind with internal audits, giving management time to implement each aspect," Schandl says. "Try to have a seat at the table throughout as management plans its approach to each stage of the law."

Understand that ACA issues are not only concerns of the HR or benefits departments. "We highlighted the importance of coordinated, regular communication between HR and benefits and the many other stakeholders that need to be informed or consulted with," Vincenti says. "An objective of the risk assessment was a robust inventory of all the implications of the ACA, which helped in categorizing them by ownership."

Be prepared to do battle with an unknown foe. "The most challenging part is that you're already into a process and your guidance is still being communicated," Gipson points out. "As some of that guidance is finalized, you may have to go back and make adjustments. That's a challenge to internal audit and the compliance team, both of which have to understand the state that is and the state that could be."

Find out what your resources are. "The first step is to talk to your HR department or benefits function and ask whether the organization uses a benefit information system that has an ACA module," Mowery says. "If the answer is no, that raises a big red flag.

The right approach to preparing for the ACA should make auditing for compliance fairly routine.

"We worked closely with our legal and compliance offices to ensure we had a correct understanding."

Gwendolyn Skillern

VISIT InternalAuditor.org's "ACA Health Check" to learn more about health-care industry auditors' approach to the U.S. Affordable Care Act.

If the answer is yes, the next question concerns a commitment by providers to complete the necessary paperwork to comply with the law. Those are the kinds of things internal audit should be concerned about."

Make sure you have a working understanding of what's expected. "You have to have some basic understanding of the regulations," Skillern urges, "and any operational and financial implications to your company if you don't comply. When the business units have questions, you want to ensure that the audit staff is knowledgeable." You can't just turn it over to the insurance company. "We worked closely with our legal and compliance offices," Skillern adds, "to ensure we had a correct understanding."

Let management do its job first. "We haven't discussed what to audit next," Schandl reports. "We probably won't consider any audits until the middle of calendar year 2016. We want to make sure management implements the appropriate processes, then allow them four to six months to have it up and running—and then test."

Pick your battles. "I would go where the fire is burning," Vincenti suggests, "meaning I would focus on anything that is coming up on a deadline. Then trace your way back to identify the owner of the process and do a quick validation that everything is ready and in place for things to go smoothly." When all the deadlines have been looked at, she advises conducting an intermediate "lessons learned" reviewer with management. "Step back for a minute and reassess your plan," she says.

Be realistic about what you can accomplish. "Don't try to swallow the whole thing in one bite," Schandl explains. "If you have a team of auditors, break the ACA up into pieces and give each person an area to be an expert in rather than trying to tackle it all." She notes that even as a CAE, she doesn't know every aspect of the act.

Get outside help when you need it. "We have a number of cosource internal audit relationships with the big firms," Skillern reports. "We used them very strategically on complex issues where we wanted the benefit of their subject-matter expertise and insight across multiple insurers." One example: There are many claims aggregation and reporting requirements tied to Centers for Medicare and Medicaid Services technology. "We partnered with a company that had auditors with experience with that type of technology," she adds. "Internal audit shops don't have the resources to have every type of expertise on staff." Mowery agrees: "I'd really recommend using subject-matter experts at least in the initial audits because of the highly technical nature of the regulations. A number of systems will be involved in getting the reporting requirements together, including payroll and a benefits module, and you really need to understand the whole flow."

A SMART APPROACH

The right approach to preparing for the ACA should make auditing for compliance fairly routine. "We're not involved right now," Schandl notes. "We're talking about it. We'll determine where the biggest concerns lie, perform a risk assessment and then build an audit calendar around that." Vincenti is similarly sanguine. "It's been a full year of execution under the ACA, and my team and I have not even gone to look at it," she says. "We haven't heard anything." Is she surprised? Hardly. "A lot of the work was done ahead of the game," she says. "The ACA is not considered a high risk anymore. Believe me, I have so many other things to do that pose bigger risks." IA

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

Powerful Insights. Proven Delivery.®

A Global Look at IT Audit Best Practices

There is no disputing technology's role in business today as an enabler of virtually every process and function. With this enablement and the advantages IT brings also come global risks – security, cyberattacks, privacy issues, data breaches, governance, asset management and much more. The critical question we ask is: Are IT audit practices keeping pace in order to assess, monitor and mitigate critical risks coupled to a technology-enabled business? This is what ISACA and Protiviti set out to determine in conducting the fourth annual *IT Audit Benchmarking Survey*.

Download a copy at **protiviti.com/itauditsurvey**

protiviti®
Risk & Business Consulting.
Internal Audit.

For at least the past decade, internal auditing has been in a state of growth and progressive change. And while it has evolved and advanced significantly, many practitioners nonetheless remain bound by some fundamental, confining paradigms. These paradigms include:

- Internal auditors plan, execute, and report results of point-in-time audits.
- Internal auditors assess internal controls and report opinions on whether they believe controls are effective.
- Internal auditors report what they believe to be control deficiencies, material weaknesses, significant deficiencies, or opportunities for improvement.
- Direct-report auditing is the primary approach used globally. In a direct-report engagement, the auditor evaluates the subject matter for which the accountable party is responsible. The accountable party does not make a written assertion on the subject matter.
- The profession has been primarily supply-driven rather than demand-driven, as boards and C-suites have often not specified their assurance needs—leaving internal audit departments to form their own views regarding which objectives/topics to focus on.
- Internal audit often does not know, or require that management and boards define, the type and amounts of residual risk the company and its board are prepared to accept.

REINVENTING internal audit

Tim J. Leech

Recent governance-related developments require the profession to revisit some of its long-held paradigms.

- Many internal audit departments have not assessed and reported on risks to the organization's top strategic/value-creation objectives, or the effectiveness of its overall risk management framework. According to Enhancing Value Through Collaboration, an IIA Pulse of the Profession report, internal auditors surveyed dedicated a mere 8 percent of resources to their company's strategic objectives in 2014.

The profession's long-established practices have generally been viewed as adequate—even good to excellent—but their relevance to today's stakeholders has begun to diminish. A shifting governance landscape places the profession's traditional methods in jeopardy and points to the need for radical change. As stakeholder expectations evolve, internal audit must revisit existing paradigms and rapidly adjust to maintain its relevance.

GLOBAL DEVELOPMENTS

Key developments over the last several years have significant implications for boards, senior management, and, in particular, internal auditing. The changes they've brought span across industries and geographical boundaries, and are far-reaching in scope.

Increased Board Risk Responsibility Following the 2008 global financial crisis, commissions were convened around the world to help understand what had gone wrong and prevent destabilizing events in the future. From these efforts, consensus emerged that boards and, to a lesser degree, regulators, had not adequately discharged their duty to oversee what is increasingly being called management's "risk appetite and tolerance." Consequently, board responsibility for overseeing management's risk appetite and tolerance has risen significantly.

Creation of the Financial Stability Board Shortly after the onset of the global financial crisis, the Group of Twenty, an assembly of representatives from the world's largest economies, created a new international regulatory advisory body—the Financial Stability Board (FSB). The board currently includes government officials and financial sector and securities regulators from around the world. With unprecedented speed, it has formulated and disseminated paradigm-shift guidance that could effectively spur the reengineering of corporate governance globally.

Among the FSB's most significant contributions to date is a November 2013 guide for national regulators, companies, and auditors titled Principles for an Effective Risk Appetite Framework. The guide's authors define new and bold proposals for management, boards, and internal auditors. Details of the role proposed for internal auditors are shown in "FSB's Guidance for Internal Audit" on page 48. In essence, the FSB calls on practitioners to transition from providing point-in-time, direct-report, subjective opinions on control effectiveness for a small percentage of an entity's risk universe to reporting on the reliability and effectiveness of an organization's entire risk appetite framework. The scope of reporting would include the reliability of enterprise risk status reports provided to the board by senior management. Although the FSB framework was aimed primarily at the financial services industry, the core concepts it promotes are relevant to all sectors.

Adoption of FSB Guidance Regulators around the world have started to enact regulations that reflect key FSB recommendations—particularly the need to assign primary responsibility for risk management and reporting to management; and risk appetite and tolerance oversight to boards. The revised U.K. Corporate Governance Code, issued in September 2014, provides one of the most notable illustrations of this activity. It positions responsibility for risk oversight squarely with boards of directors; calls on management to design, implement, and maintain effective risk governance frameworks; and asks boards to seek independent assurance that management has designed, implemented, and maintained effective risk governance frameworks. Other countries that want to improve the integrity of their capital markets are expected to follow the U.K.'s lead.

> **The revised Corporate Governance Code positions responsibility for risk oversight squarely with boards of directors.**

Reduced Audit Client Satisfaction As these regulator-driven developments gain traction globally, PricewaterhouseCoopers' 2014 State of the Internal Audit Profession Study paints a picture of a significant decline in board and senior management satisfaction with traditional, direct-report internal audit services. One of the report's most disturbing findings is that half of senior management and nearly 28 percent of board members

FSB'S GUIDANCE FOR INTERNAL AUDIT

In its Principles for an Effective Risk Appetite Framework, the Financial Stability Board proposes specific responsibilities for internal audit and other independent assessors. The framework states that internal audit should:

- Routinely include assessments of the risk assessment framework (RAF) on an institutionwide basis as well as on an individual business line and legal entity basis.
- Identify whether breaches in risk limits are being appropriately identified, escalated, and reported, and report on the implementation of the RAF to the board and senior management as appropriate.
- Independently assess the design and effectiveness of the RAF periodically, as well as its alignment with supervisory expectations.
- Assess the effectiveness of the implementation of the RAF, including linkage to organizational culture, as well as strategic and business planning, compensation, and decision-making processes.
- Assess the design and effectiveness of risk measurement techniques and [management information systems] used to monitor the institution's risk profile in relation to its risk appetite.
- Report any material deficiencies in the RAF and on alignment (or otherwise) of risk appetite and risk profile with risk culture to the board and senior management timely.
- Evaluate the need to supplement its own independent assessment with expertise from third parties to provide a comprehensive independent view of the effectiveness of the RAF.

say internal auditing adds less than "significant value" to their organization. Moreover, only 49 percent of senior management and 64 percent of board members say internal auditing is delivering on expectations.

IMPLICATIONS FOR INTERNAL AUDITING

The changes described are causing regulators, boards, and senior executives to reconsider and reshape what they want and expect from internal audit. What once constituted fine, even laudable deliverables from internal audit in the minds of many boards, C-level executives, and regulators is being reshaped by increasing expectations that internal audit play a key role in helping boards demonstrably oversee management's risk appetite and tolerance.

Risk Reporting The FSB has defined roles for the board, senior management, and internal audit that call for a fundamental accountability shift—a shift that would require management to continuously assess and report upward on risk status. Moreover, it would require internal audit to help management build and maintain systems for this purpose, as well as assess and report opinions to the board on how well management is discharging its assigned risk governance responsibilities. This new paradigm requires fundamental shifts in existing internal audit educational resources. The IIA modified its Performance Standard 2120: Risk Management in 2010 specifically to provide support for the shift, and in 2012 it also began offering the

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

Certification in Risk Management Assurance designation globally.

Internal audit departments that aren't doing so already need to evolve beyond the business of performing traditional, point-in-time, direct-report audits and providing subjective opinions on "control effectiveness" for a small percentage of their organization's total risk universe. Instead, they need to focus substantially more resources on providing assurance to boards that senior management is creating and maintaining what is increasingly being referred to as an effective risk appetite framework.

Educating the Board Regulatory, director, senior management, and common law expectations are likely to evolve at varying speeds and intensity in different countries. Not all senior management and board members have been actively following the evolution of these expectations, and not all national regulators — including the U.S. Securities and Exchange Commission — have codified risk governance expectations with the clarity and simplicity of the 2014 U.K. Corporate Governance Code to spur the needed transition. Moreover, not all CEOs and chief financial officers are likely to welcome direct responsibility for creating and maintaining effective risk appetite frameworks and providing formal and candid reports on enterprise residual/retained risk status to their boards — especially those outside the financial services industry, on which the FSB framework is focused.

Some CEOs may be particularly upset with the FSB recommendation that internal audit report to boards on the reliability of the organization's risk appetite frameworks and, especially, CEO/senior management reports to the board on enterprise risk status. Nonetheless, internal audit needs to ensure boards and senior management are aware of these developments and the global push to hold boards and the C-suite more accountable for overseeing management's risk appetite/tolerance.

New Competencies If internal auditors are to assume the type of responsibilities defined by the FSB, the Financial Reporting Council, and other national regulators that elect to follow the U.K.'s lead, they must retool their knowledge and skills. Instead of emphasizing opinions on control effectiveness, internal auditors must be able to assess and report on the reliability of management's risk appetite framework, including CEO/management reports to the board on enterprise retained/residual risk status. Making this transition involves learning the type of vocabulary defined by the FSB in its Principles for an Effective Risk Appetite Framework guidance and the International Organization for Standardization's ISO 31000 and ISO Guide 73.

Internal auditors should also monitor closely the enterprise risk management framework update currently under development by The Committee of Sponsoring Organizations of the Treadway Commission (COSO), scheduled for completion in late 2016. One of COSO's stated reasons for the update is to respond to escalating risk governance reporting requirements.

Auditors will also need to gain the knowledge and skills required to identify the organization's full range of risks and risk treatments linked to key objectives, and obtain a picture of residual risk status — as opposed to the much narrower assessment of traditional internal controls dimension on which internal audit has historically focused. More importantly, internal auditors need to continuously assess and report on whether the current residual risk status related to key strategic and foundational objectives is currently within the board and senior management's risk appetite and tolerance — assuming internal audit has been provided with enough information from the board and C-suite to take on this task. Internal audit can also play a key role in alerting boards to risk acceptance situations that warrant active discussion with senior management and the board.

The internal audit profession needs to reinvent itself to satisfy key customers — particularly board members.

THE NEED FOR CHANGE

Quantum change in the current internal audit paradigm will be needed to address shifting client and regulatory demands. And while human nature is to resist radical change in favor of smaller, more incremental steps, meeting these demands will require internal audit to adapt quickly. The well-known adage "necessity is the mother of invention" applies well to current circumstances: The internal audit profession needs to reinvent itself to satisfy key customers — particularly board members. Change of this magnitude constitutes no small task to be sure, but it's imperative for ensuring the future of the profession. ia

TIM J. LEECH, CIA, CCSA, CRSA, FCPA, *is managing director at Risk Oversight Solutions Inc. in Oakville, Ontario, and Sarasota, Fla.*

Enterprise Risk Services | CEO/CFO Certification Services | Internal Audit Services
Corporate Governance | **Technology Risk Services** | Business Resilience Services

MNP LLP

CYBER SECURITY

Are You Protected?

From big data to outsourcing and services provided in the cloud, today's connected and global networks present complex challenges for IT and security professionals to manage. You recognize that traditional models of protecting your perimeter network systems are no longer sufficient, but may not know where to turn for the best solutions.

MNP delivers tailored and risk-based cyber security programs to help you continuously monitor your organization, protect your services and information and ensure you can recover from a breach. With the right strategies, you can rest assured your stakeholder confidence, data integrity and reputation are protected.

How effective is your cyber security operation?

Trac Bo, Technology Risk Leader
trac.bo@mnp.ca or 403.537.8396

Professional SKEPTICISM

Skepticism has a big influence on an internal auditor's ability to approach an engagement objectively.

Rebekah A. Heath
Tim Staggs

Crucial to an internal auditor's ability to complete any audit successfully is his or her ability to demonstrate objectivity in both the approach to and performance of the engagement. Yet this may be the most difficult ability to develop and maintain, particularly because most internal auditors are employees of the organizations they audit. This potential for bias remains true even when organizations rely on outsourced service providers to perform internal audit responsibilities.

To provide an organization's management and board of directors with an audit product that meets their expectations for quality, internal auditors must be able to exercise professional judgment free from the interference that can sometimes result from their employee—or service provider—relationship with the organization. Professional skepticism is a key element of objectivity. Like most skills auditors should seek to cultivate, the ability to approach each audit engagement with the appropriate degree of professional skepticism must be intentionally nurtured through education and practice.

VIEWPOINTS ON SKEPTICISM

Standard 1100: Independence and Objectivity of The IIA's *International Standards for the Professional Practice of Internal Auditing* (*Standards*) refers to objectivity as "an unbiased mental attitude" that "requires that internal auditors do not subordinate their judgment on audit matters to others." *Sawyer's Guide for Internal Auditors*, 6th edition, echoes this definition by stating that objectivity "is the impartial, unbiased attitude that all internal auditors must have in performing

their work." Yet maintaining such an attitude, while performing engagement responsibilities effectively, is no easy task, and it depends on the development of numerous related skills such as critical thinking, self-evaluation, and interpersonal communication.

The definitions in the *Standards* and *Sawyer's* view professional skepticism as being neutral with regard to an individual's approach to auditing. In this view the internal auditor neither assumes that management is dishonest nor assumes unquestioned honesty—he or she simply has a questioning mind and critically assesses audit evidence. This "neutrality" view of professional skepticism anticipates that auditors are able to separate themselves from those external and internal biases that could negatively affect their ability to evaluate the audit evidence objectively. However, this view often leaves unanswered questions about how auditors can determine when they have effectively exercised skepticism in their audit approach or how to measure the possible effect on the evaluation of audit evidence whenever they have not.

On the other hand, standards that focus on fraud, such as U.S. Public Company Accounting Oversight Board standard AU Section 316A, Consideration of Fraud in a Financial Statement Audit, take a forensic-audit view of professional skepticism in which auditors have an attitude of "presumptive doubt" and assume some level of dishonesty by management, unless the evidence indicates otherwise. For internal auditors, such an approach may be applicable when considering the possibility of fraud in all types of audits.

Under a presumptive doubt view, auditors possessing a high level of professional skepticism are more likely to doubt the sufficiency of evidence that would normally be viewed as appropriately supporting the audit objective. Such auditors will tend to collect more evidence, which may result in a less efficient audit.

As reliance on the work of internal audit by external parties grows, internal auditors should note that regulators appear to take the presumptive doubt perspective of professional skepticism. Regulators typically cite professional skepticism as a missing ingredient in the auditor's objectivity whenever an external audit failure has occurred. The U.S. Securities and Exchange Commission often has identified a lack of professional skepticism as a primary contributing factor to the circumstances involved in enforcement cases, as well as in malpractice claims against external auditors.

Internal auditors should be prepared to defend their level of objectivity.

Likewise, law enforcement agencies tend to refer to external audit standards in fraud cases. With this in mind, internal auditors should be prepared to address, or defend, their level of objectivity in completing an audit that is to be relied on by others or that is the basis of an external investigation. To do so, internal auditors must be able to understand, identify, and approach such engagements with an appropriate level of skepticism.

A SKEPTICISM CONTINUUM

Professors Stephen Glover and Douglas Prawitt of Brigham Young University propose a different view on the exercise of professional skepticism in a 2013 publication from the Center for Audit

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

49% of respondents say their board and management practice tactful skepticism in their respective roles, but 30% disagree, according to a January 2015 IIA *Tone at the Top* poll.

DIVERGENCE AND CONVERGENCE

Professors David Plumlee and Brett Rixom of the University of Utah, and Andrew Rosman of the University of Connecticut, view professional skepticism not as a trait or mind-set, but rather as a diagnostic-reasoning process that is found in the problem-identification and structuring phases of creative problem-solving. In a 2011 study funded by the Center for Audit Quality, the researchers found that providing online training to senior auditors that taught them to reason diagnostically improved their ability to be professionally skeptical. Specifically, the auditors were given less than persuasive evidence and were asked to use divergent thinking followed by convergent thinking when evaluating the evidence.

Divergent thinking requires auditors to generate explanations for evidence or circumstances they identify as unusual without a concerted effort to ensure that each explanation is logically valid. Once they have produced a complete set of explanations, auditors use convergent thinking to systematically assess the plausibility of each of them. Plumlee and his colleagues found that divergent thinking training increased both the number and quality of explanations generated for an unusual situation. In addition, those senior auditors trained in both divergent and convergent thinking were more likely to generate and ultimately choose the correct explanation compared to those who did not receive the full training.

The researchers hypothesized that the typical mode of generating explanations involves a continuous examination of possible explanations known as "consistency checking." Moreover, they posited that auditors who were trained to apply a sequence of divergent thinking followed by convergent thinking will not resort to "consistency checking." Decision-makers spontaneously engage in consistency checking when they evaluate explanations as they occur, eliminating some based on superficial consideration. Training in both types of thinking led individuals, during the divergent phase, to consciously keep explanations they generated for later evaluation during the convergent thinking phase of the diagnostic-reasoning process.

Quality's Global Public Policy Committee, which comprises the six largest public accounting firms. In Enhancing Auditor Professional Skepticism, they advise auditors to approach each engagement using a "professional skepticism continuum" where the appropriate level of skepticism depends on the risk characteristics of the area under audit.

On this continuum, the level of professional skepticism moves from something less than complete trust, to a neutral mind-set, to presumptive doubt, and all the way to complete doubt. The appropriate level of skepticism to apply is initially determined only after a careful and rigorous risk assessment. However, Glover and Prawitt stress that to ensure an appropriate level of professional skepticism is consistently applied to collecting and evaluating all audit evidence, the auditor should continue to reevaluate that initial determination throughout the engagement.

In using the continuum approach, less persuasive evidence is required for those instances where no fraud indicators exist, no errors are detected, routine processes requiring little judgment are examined, and the audit evidence is consistent with the initial risk assessment, regardless of the area of risk being audited. Likewise, less persuasive evidence would be required for those assertions of lower risk. This frees auditors to focus the bulk of their efforts on high-risk areas where there logically should be greater doubt.

ENHANCING SKEPTICISM

Skepticism is both a personality trait and a state of mind. Personal traits that contribute to the auditor's ability to exercise appropriate professional skepticism include a questioning mind, the ability to analyze and critically evaluate, problem-solving ability, ethical and moral reasoning, a willingness to suspend judgment, and a tendency to search for knowledge, according to a 2010 article by Baylor University accounting professor Kathy Hurtt, "Development of a Scale to Measure Professional Skepticism." Three additional abilities ensure that an individual's skeptical mind-set will translate into actions: interpersonal understanding, a sense of autonomy, and confidence based in self-esteem. Interpersonal understanding considers human biases when analyzing evidence, while autonomy and self-esteem pertain to the courage to stand up to the pressures of others and draw one's own conclusions.

In practice, academic research has shown that audit students and practicing auditors do not differ in their overall levels of skepticism, which is consistent with the theory that skepticism is a relatively stable personality trait. Developing their creative problem-solving skills is one way auditors can increase their level of skepticism (see "Divergence and Convergence" on this page).

Encouraging a skeptical mind-set may be as simple as providing fraud

training or training in the appropriate use of Glover and Prawitt's continuum. Several activities provide starting points for enhancing the professional skepticism of an internal audit team.

Skepticism affects internal auditors' ability to make sound judgments.

Improve Critical Thinking Training and other activities designed specifically to strengthen critical-thinking skills can have a positive effect on an auditor's ability to approach audit evidence with more skepticism. There are many resources available to develop such skills.

Self-evaluate Objectivity IIA Standard 1120: Individual Objectivity calls on internal auditors to "have an impartial, unbiased attitude and avoid any conflict of interest." One way to gauge potential conflicts of interest is to have team members identify relationships and other influences, such as friendships with associates in the area under audit, that potentially could have a negative effect on their objectivity. Audit leaders should evaluate the level in which these influences could affect auditors' judgment, then identify ways to counter them. The IIA Research Foundation report, Behavioral Dimensions of Internal Auditing: A Practical Guide to Professional Relationships in Internal Auditing, can be helpful in evaluating professional relationships.

Involve Auditors Outside the Engagement Team When possible, internal auditors should invite a member of the audit group who is not on the current engagement team to interview an individual, if they believe their personal relationship with that person may negatively affect their ability to be appropriately skeptical. They should observe the interview as a nonparticipant, drawing their own conclusions. Afterwards, auditors should debrief the interviewer to learn his or her conclusions and compare them to their own, evaluating whether any significant differences were the result of the degree of skepticism employed.

Post-audit Peer Reviews Internal auditors should ask colleagues to review their work on a recent audit that involved a substantial degree of judgment or tested their objectivity. Such peers should challenge them to defend the type and volume of evidence accumulated during the engagement. Then auditors and their peers should evaluate whether the evidence supported the conclusions, in light of the audit objectives, and the auditors demonstrated an appropriate degree of skepticism.

INFLUENCING JUDGMENT

Ultimately, an internal auditor's ability to maintain objectivity through the use of professional skepticism affects his or her ability to make sound judgments. But as important as skepticism is, it is only one of the factors that influence professional judgment, alongside audit and industry expertise.

As internal auditors begin their next engagement, they should consider how their view of professional skepticism will ultimately affect their evaluation of the audit evidence. They should take time to document their thought process and its effect on that evaluation. Moreover, they should keep in mind that a competent auditor is a skeptical auditor. la

REBEKAH A. HEATH, PHD, CIA, CPA, *is assistant professor of accounting at Middle Tennessee State University in Murfreesboro.*
TIM STAGGS, CIA, *is vice president of internal audit and compliance with Healthcare Realty in Nashville.*

An effective governance strategy can ensure an appropriate level of owner oversight and minimize shared risks.

Joint Venture / Joint Exposure

Ben Arnold

As the phrase suggests, a *joint venture* is a business agreement between two or more parties that choose to enter into a partnership for profit. But it also means joint exposure to adverse consequences and potentially significant exposure to the owners' objectives, particularly from a strategic, financial, and reputational perspective.

Even with less than 50 percent ownership or control, the parent company can be subject to liability if there is actual knowledge or deliberate ignorance of any inappropriate conduct. There have been numerous cases where owners have been impacted by actions within a joint venture or subsidiaries. In February 2015, the U.S. Securities and Exchange Commission (SEC) fined Goodyear Tire & Rubber Co. US$16 million after alleging its subsidiaries in Kenya and Angola bribed government officials, employees of private companies, and government-owned entities to obtain sales. The bribes were recorded as legitimate expenses in the books from 2007–2011, a violation of the U.S. Foreign Corrupt Practices Act (FCPA). Goodyear's self-reporting and cooperation in the investigation resulted in a less severe fine. In a 2011 case, London-based multinational alcoholic beverages company Diageo also was fined US$16 million by the SEC because its subsidiaries in India, South Korea, and Thailand bribed foreign government officials to gain sales and tax benefits.

In addition to financial considerations resulting from poor joint venture governance, evidence has indicated that other consequences, particularly reputational and license to operate, can have more significant impacts on the owner. Generally,

the perceived largest severe impact would be to corporate reputation, rather than legal, financial, and regulatory impacts.

The role of internal audit and risk management is vital to support management in the development and ongoing monitoring of the joint venture governance framework. Joint venture owners' audit strategy and risk management processes will require high coordination and strategic thought between the relevant owner audit departments/risk teams and joint venture teams, if applicable.

With a vast range of joint venture structures and operations across several industries (including the owner directly operating the joint venture on behalf of the owners or the joint venture having its own operating and management structure), the owner's implementation of an effective governance process can be challenging.

RISK MANAGEMENT

A typical, nonoperated owner challenge is ensuring that risk management within the joint venture is effective. Effective risk management will depend on the nature of the joint venture relationship, including level of influence, ownership/management control, and the owner's appetite for control monitoring and risk management.

Regardless of the chosen approach, the minimum requirement is an effective

THE CASE OF TSKJ

TSKJ was a joint venture formed by the U.S.'s M.W. Kellogg Co. (later became KBR), France's Technip, Japan's JGC, and Italy's Snamprogetti. The joint venture company won four contracts worth more than US$6 billion between 1995 and 2004 to design and build liquefied natural gas facilities on Bonny Island, Nigeria. None of the participants had a majority stake in the joint venture.

TSKJ used agents to bribe Nigerian government officials. The U.S. Department of Justice (DOJ) proved that TSKJ paid about US$132 million to a Gibraltar corporation controlled by London lawyer Jeffrey Tesler and more than US$50 million to a Japanese trading company, with the intention of using the money for bribes.

The DOJ and U.S. Securities and Exchange Commission (SEC) declared that each joint venture partner had culpable knowledge because senior executives from each company, including some who were serving on the TSKJ steering committee, participated in meetings in which the bribery of Nigerian government officials was discussed. The executives authorized payments to secure contracts for the company.

Together, the four multinational corporations and the Japanese trading company paid a combined US$1.7 billion in civil and criminal sanctions in 2010 for the decade-long bribery scheme. These include:

- Snamprogetti and its parent company ENI agreed to pay US$365 million to resolve charges related to the U.S. Foreign Corrupt Practices Act (FCPA) for Snamprogetti's role. The financial penalties included a US$240 million criminal fine to the DOJ and US$125 million in disgorgement to the SEC.
- Technip resolved FCPA-related charges with the DOJ and SEC for US$338 million, including a US$240 million criminal penalty and US$98 million in disgorgement.
- Consortium leader KBR and its former parent Halliburton paid US$579 million to settle FCPA-related charges, including a US$402 million criminal penalty and US$177 million in disgorgement.

Nonfinancial impacts in this case included reputational damage and criminal charges against current and past joint venture parent employees. In addition, KBR's FCPA violations impacted successor liability after Halliburton acquired KBR in 1998 (it later sold KBR in 2007). These were based on book and record violations and Halliburton's lack of post-acquisition vigilance. On the financial side, the FCPA and U.K. Bribery Act investigations also affected share price and capitalization.

68% of respondents expect their companies' joint venture activity to increase over the next five years, according to a 2014 McKinsey & Co. survey of C-level and senior executives.

risk and control monitoring process by both the owners and operators. The joint venture operator may have implemented a formal risk management program, including risk analysis, control assessments, and monitoring; however, the minimum requirements should include implementing a risk-proportional risk management process by both the owner and operators, which will give owners an adequate comfort level over the joint venture.

Embedding a risk management process allows the owner to structure governance processes and understand the risk exposures and control effectiveness relating to joint venture operations. In addition, monitoring risk management processes and connecting joint venture risks can provide owners with necessary insight into the potential for exposure.

The implementation and ongoing monitoring of a risk management process will depend on several factors. A key aspect is the area of ownership control versus influence. Existing tools and methods are used to determine control for legal and financial reporting purposes (e.g., greater than 50 percent joint venture ownership would normally indicate control); however, risk exposure in joint ventures should be managed based on the breadth and areas of risk impact.

EXPOSURE LEVEL

A critical aspect of joint venture governance is determining the level of exposure that joint venture operations may have on the achievement of the owner's strategic objectives. In other words, is the joint venture a financial investment, does the owner have "skin in the game," or are there additional nonfinancial consequences or financial impacts greater than the investment value if things go wrong? Potential consequences surrounding a financial investment are generally limited to financial exposure; however, if the joint venture is more than a mere financial investment, additional consequences such as reputational, community, environmental, and strategic risk impacts may materialize.

Is the strategy achievable, considering the relative risk maturity of all parties?

Some key points for management, internal audit, and risk management to consider when determining governance strategy include:

- **Risk process.** Is an effective risk management process in place (and in larger organizational settings, does the process include a dedicated risk management team)? Is the risk process aligned with the owner's process or best practice?
- **The availability and maturity of risk monitoring information.** The ability to obtain and analyze information provided by the joint venture will depend on influence (e.g., strength of relationships between the joint venture and owners) or the embedding of monitoring and information provisions within it (e.g., formal requirements included in agreements for governance and provision of information).
- **The risk maturity of both owner and joint venture.** Is the strategy achievable, considering the relative risk maturity of all parties? The risk management framework should consider risk awareness and control monitoring at the joint venture level.
- **Risk culture.** Will the organizational culture within the existing joint venture governance process support effective risk management? Key enablers or indicators can include tone at the top, communication between joint venture and owners, and creation of risk or governance committees.
- **Commercial sensitivity (anti-trust).** Will the provision of information between the joint venture and owners align with anti-trust requirements? What are the controls in place to ensure that the joint venture and owners appropriately maintain commercially sensitive information?
- **Continuous control monitoring and provision of information.** Regardless of the strategy selected, the control monitoring performed by the owner should be designed to ensure the provision of timely and accurate data. Ideally, the control design and feedback will allow the risk and control owner to understand whether the control is about to fail (i.e., leading indicator) rather than following a control failure (i.e., lagging indicator).

A JOINT VENTURE CASE STUDY

Given the realization of joint exposure, the implementation of a risk-proportional risk and audit process will enable the owner to gain adequate comfort over joint venture operations. The process to develop the strategy from inception was explored by fictional Company XYZ.

Company XYZ is a 50/50 owned joint venture. Both joint venture partners are industry owner-operators with separate management and operational structures. The joint venture board includes representatives of the owners

and members from the joint venture company management team.

While legal and accounting interpretations of the joint venture structure indicate that owner No. 1 does not control operations at the company, significant risk exposures to owner No. 1 were identified during the board governance process. During a risk strategy session, two options were identified to implement a risk-proportional risk management process.

Joint ventures can cause significant exposure to the owner's objectives.

OPTION 1

- The joint venture maintains the risk profile and communicates it to owner No. 1 periodically. The company completes control monitoring through internal processes.
- Company XYZ risks included in owner No. 1's risk profile are based on percentage of ownership and impact. No specific risk monitoring is performed or formalized by owner No. 1.
- Generally, the financial impact of risks is to be calculated based on owner No. 1's equity ownership (50 percent), and other impacts (reputational; health, safety, environment; and legal) are included at 100 percent.

The advantages to this arrangement are fewer dedicated resources with a focus on the joint venture company risk management process and reliance on existing processes. However, the disadvantages are the lack of ownership and risk monitoring performed by owner No. 1, the risk profile not necessarily representing owner No. 1's view or assessment, and the inclusion of a high number of operational risks within owner No. 1's profile.

OPTION 2

- The joint venture company's material risks are individually assessed and included directly from owner No. 1's perspective within the established risk management process.
- The risk ratings will be decided based on work completed by the joint venture entity, but can be different depending on the effectiveness of owner No. 1's control or perspective.
- Owner No. 1's operational management governance hierarchy is the primary owner of risk and control.

The advantages of this option are an accurate reflection of the joint venture (owner) risk profile, appropriate governance and accountability residing with owner No. 1's risk and control owners, and the ability to enhance a balanced control-monitoring process. The disadvantages, however, could include initial increased efforts to develop and embed the risk process and supporting internal control and governance frameworks.

Following review and consultation by all stakeholders, owner No. 1 identified Option 2 as the preferred risk management process. However, this approach required the identification and formation of the risk profile, with consideration of several key factors.

Ownership Given the absence of existing defined risk management roles with owner No. 1, decisions around risk and control ownership were informed

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

51% of CEOs plan to enter into new strategic alliances or joint ventures over the next year, up from 44% in 2014, according to PricewaterhouseCoopers' 2015 annual Global CEO Survey.

based on the existing governance structure and oversight from owner No. 1. Through the risk management process, the level of governance and oversight would be generally formalized and enhanced by detailing owner No. 1's risk and control responsibilities.

Risk Profile The risk events within the owner's risk profile can be articulated in several ways and need to be consistent with the remainder of the risk profile to ensure a consistent and comparable process. Generally, the owner's risk profile for the joint venture could include a blend of:

- **1:1 Risk.** Significant risks that might coexist on the joint venture risk profile require both owner and joint venture control monitoring due to the implication of the risk and impacts.
- **Consolidated Risk.** Owner risks that consolidate or merge subordinate joint venture-identified risks will reflect the appropriate risk elements, but allow the ability to focus the owner control monitoring on joint venture governance and monitoring, rather than on the more detailed control monitoring in 1:1 risk.

Performance Metrics The performance metrics developed for the owner's risk will likely be different from the joint venture risk metrics, so different strategies will need to be used. Typically, the metrics from the owner's perspective will be at a higher level than the joint venture operational controls, with a focus on monitoring and joint venture oversight. One example of owner metrics could involve performing periodic review of the joint venture operations risk management process. However, the joint venture operations metrics could involve monitoring directly related to the risk, such as ratings, critical control performance, action tracking, and event monitoring. These metrics will be incorporated within the risk and control documentation to ensure correct focus by the owners.

Risk Documentation and Criteria Risk documentation must be developed to reflect the minimum requirements for the intended monitoring that owner No.1 performs. An example of risk monitoring criteria for the two different types of risk could include:

- **1:1 Risk.** Operational monitoring directly related to the risk, including assessment ratings, performance metrics, and remediation or issues tracking; and oversight of key risk and control performance through the joint venture's risk and critical control owners.
- **Consolidated Risk.** Periodic review (a minimum of every six months) of the overall joint venture risk management program/process by a nominated risk or audit professional. Ongoing monitoring of joint venture risk management action tracking (e.g., remediation tasks or audit findings) related to potential failure of causes for owner No. 1's risks.

Provision of Information Concurrent strategies should be considered to obtain the necessary data for owners' control information and monitoring needs. By formalizing monitoring by owner No. 1, new and more frequent information flows may be necessary with mechanisms in place to ensure that information provided is timely and accurate. A key consideration is that any information provided between the joint venture and owners, especially commercially sensitive information, is in accordance with relevant anti-trust regulations.

Audit Approach/Verification Before implementation, obtaining owner alignment on the audit approach and inspections is critical. Internal audit will need to decide about timing, coordination, and co-participation, and important areas of audit scoping and criteria will need to be decided. The owner and joint venture should determine whether the audits will be measured against joint venture procedures, owner's procedures, or best practice. Ideally, these will be aligned; however, when there are differences, there needs to be consultation among joint venture and owner's management and governance teams on the agreed reference points for appropriate risk management and control monitoring.

LESSEN EXPOSURE

Joint ventures can cause significant exposure and adverse consequences to the owner's objectives, even with the absence of owner control. Implementing a risk-proportional risk management process will maximize the opportunity to achieve both joint venture and owner strategic objectives. Risk management and internal audit should be active in joint venture governance, from thought leadership and support during governance strategy development to control monitoring, execution of joint venture audits, and follow-up.

Developing the right audit and risk process will include thought and definition around the correct risk and exposures from the owner's perspective and the implementation of risk performance criteria and monitoring. Ongoing, continuous monitoring throughout the process, supported by risk and audit, will be vital in ensuring that owners have an appropriate level of oversight and, ultimately, comfort over joint venture operations. IA

BEN ARNOLD, CIA, CA, CFE, CGAP, *is principal of risk and governance for BHP Billiton Iron Ore in Perth, Australia.*

Governance Perspectives

BY MARK BRINKLEY

THE SERIOUS TONE OF WHISTLEBLOWING

Organizations should be structured to enable reporting of wrongdoing without fear of reprisal.

The U.S. Securities and Exchange Commission (SEC) issued its 2014 Annual Report to Congress on the Dodd-Frank Whistleblower Program in November 2014. The report indicates last year was "historic" regarding the number of reports, resulting in a banner year for whistleblower awards. In 2014, the SEC's Office of the Whistleblower received 3,620 tips, up from 3,001 in 2012 and 3,238 in 2013. Countries with the most reports include Australia, Canada, China, India, the U.K., and the U.S.

Internal auditors should pay attention to this report to help further corporate governance practices. Governance processes should not only promote reporting internally, but ensure strong follow-up with the reporters. Furthermore, if a report does reach the SEC whistleblower program, the organization should envelop the employee with support to protect against additional fines and penalties.

The SEC report notes that more than 40 percent of those who received monetary awards were either current or past employees of the organization they were reporting. Of this 40 percent, more than 80 percent had raised their concern via an internal reporting channel before reporting to the SEC.

Creating an ethical culture requires diligence around communication, training, and reinforcement. Compliance teams must not waste this training effort with slow or nonexistent follow-up on reports. The Office of the Whistleblower responds to questions within 24 hours. Organizational policies should mirror this practice.

Tracking the progress, timeliness, quality, and outcomes of reports must be part of any investigation. An open channel of communication with the whistleblower is key to a timely conclusion of the investigation.

A 2014 benchmark report prepared by NAVEX Global notes the median number of days to close an internal whistleblower case increased from 30 to 36 days. The longer the corporate investigation, the more likely it is there will be more reports.

Often, the investigator will pose additional inquiries regarding the situation. Increasing awareness of the need for the whistleblower to respond timely to follow-up questions is becoming apparent. Improving corporate training practices and awareness of the follow-up component is critical.

In June 2014, the SEC brought its first enforcement action against an employer who retaliated against a whistleblower. In this case, the whistleblower was demoted, and the person's scope of authority was reduced; however, compensation was not affected. The SEC fine was in excess of US$2 million. Addressing employee anxiety,

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

as well as training employees to recognize it, must be a priority. Recognizing acts of retaliation, such as sudden, clustered, or improperly documented disciplinary actions, is critical.

The SEC is making it clear that the company is not to interfere with an employee's ability to report alleged wrongdoing. The chief of the Office of the Whistleblower has publicly said that the SEC is "looking for the first big case here." Review of severance policies and agreements should be the first step in ensuring compliance with this enforcement practice. These agreements often have penalties for any negative comments by the terminated employee.

It takes courage to report potentially serious violations by an individual's co-workers or senior management. Whistleblowing, at a minimum, can have an emotional impact on the reporter. At worst, it can lead to the whistleblower's firing, suspension, or seclusion, as well as suspicion that creates factions within the organization. Regular, at least annual, mandatory training regarding the organization's whistleblower and nonretaliation policy should be conducted. Awareness is critical.

It is time for internal audit to enhance corporate awareness efforts and practices:

- Ensure all staff clearly understand their duty to report *and* provide assurance of the no-retaliation policy.
- Reinforce that message through culture change driven by periodic policy reviews and informal discussions at team meetings. This may require tools and talking points to ensure consistency in message. The key is redundancy through repetitive messaging.
- Train leaders on how to receive even slight reports or rumors with assurance that whistleblowers are valued.
- Test the reporting process to ensure its efficacy. The test should ensure expediency of the investigation, that reporting metrics are well-defined and consistently reported, that retaliation is not tolerated, that training supports this pillar, and that all reporters are respected.

Whether the organization is small or large, local or multinational, public or private, the culture of governance is driven by each employee. Ensure your organization has the correct structure to enable whistleblowers to report wrongdoing. la

MARK BRINKLEY, CIA, CFSA, CRMA, *is the director of grants at the Kauffman Foundation in Kansas City, Mo.*

Many Fortune 500 companies count on The IIA's On-site Training to develop their team's skills. **Join them today!**

You're only as good as your team.

You know you have a great internal audit team. Are they perfect? No. But they are there for you — day in, day out. When challenges arise, they have your back.

And now is your opportunity to have theirs. Thank them for their hard work and show them that you are as committed to their professional development as they are. Because let's face it — **when your team shines, you shine.**

Are you ready to shine?

Contact us today and let us help develop your plan to enhance your team's performance through in-house training. Our consultants will work with you to understand your business, your people, and the learning outcomes you want to achieve.

+1-407-937-1388 ■ GetTraining@theiia.org ■ www.theiia.org/onsite

The Institute of Internal Auditors

2015-5023

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

BY J. MICHAEL JACKA

THREE HIGH-RISK AUDITS YOU MAY BE IGNORING

Auditors seem to avoid certain areas of concern, even when clients specifically draw attention to them.

An auditor walks into a bar. He tells the owner, "I am here to help you. What are your biggest risks; what keeps you up at night?" The owner replies, "My biggest risk is that bartenders may serve underage drinkers. This represents a significant compliance, financial, and reputational risk for my bar." The auditor, pleasantly surprised to hear such a knowledgeable owner, says, "Thanks—I really appreciate the input. So, let's start with an inventory count."

It doesn't take much effort to learn what our clients consider their biggest risks. However, we seem to avoid certain areas—even when clients express specific concern about them. One reason may be that we have not made the connection between the risks and the process. But it also might be that we find the process hard to define, we don't think it is part of our audit universe, or we're just a little afraid to go into unknown territory.

There are three risk areas our clients consistently rate as significant: reputation, human capital, and money. Nonetheless, internal audit seldom explores certain areas that impact those risks significantly.

Ethics Across organizations and industries, ethics is foundational to risk and control frameworks, and it is at the core of reputation. Even the fallout from episodes like the 2010 BP oil spill in the Gulf of Mexico was as much about perceived ethical lapses as it was the spill itself. Yet few auditors even consider the impact of ethics in individual audits. And while ethics is hard to define and hard to test, difficulty should never be the cause for us to ignore a risk.

Human Resources Depending on an organization's structure, human resources can oversee everything from hiring to development to personnel policies to anything else that touches on human beings. To complicate matters, human resource departments are not accustomed to being reviewed and may be somewhat protective of the sensitive information they handle. But the most important resource of any organization is its people, and we have a responsibility to provide assurance that this resource is protected and developed.

Marketing Where does all the money go? For most organizations, anywhere from 5 to 15 percent of revenue is spent on marketing activities. Some audit functions have made forays into this area by performing reviews of advertising—often doing little more than making sure payments match the bills. But there is a lot more to marketing than just the ads. Upon review, auditors will encounter unfamiliar concepts and jargon that may confuse more than confirm. But this isn't a reason to shy away from an area that significantly impacts the money spent on the organization's brand and reputation.

If I am wrong—if you have taken the plunge and are creating impactful results in these areas—please let me know. But I think most auditors are still living in denial, fear, ignorance, or a little bit of all three. 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

THE FUNCTIONAL SMALL AUDIT DEPARTMENT

With the right approach, these functions can provide as much value as their larger counterparts.

ROBERT KASTENSCHMIDT
National Leader
Risk Advisory Services
McGladrey LLP

WILLIAM WATTS
Partner in Charge
Business Risk Services
Crowe Horwath LLP

How do you define a *small* audit function?

WATTS Typically, small audit functions have fewer than six auditors, limited or no use of technology—such as a GRC tool or data analytics technology—and no full-time or limited specialty skills.

KASTENSCHMIDT While head count is one indicator, a small audit function is more accurately defined relative to the size of its mission. A function is "small" for its organization if it struggles with its ability to identify and adequately address relevant risks. In my mind, the audit function includes all of the resources controlled by the CAE, including both internal staff and external resources.

In light of their size, what are the biggest risks small audit functions face in providing adequate coverage/service to their stakeholders?

KASTENSCHMIDT The biggest risks include:

- Developing audit plans that reflect the internal audit team's capabilities rather than the organization's business risks.
- Unintentionally providing a false sense of security by underauditing relative to the level of comfort that the audit function communicates to stakeholders.
- Failing to clearly articulate the intended role of internal audit within the organization, thus diluting audit's impact by trying to meet undefined—and often conflicting—stakeholder expectations with very limited resources.

WATTS Usually three areas pose the greatest challenge to small internal audit functions. The first area is footprint or capacity. Getting risk coverage with limited resources can create gaps in risk mitigation, or an inability to handle all key risks. There is only so much bandwidth to cover all needs.

The second area is skills and experience. To meet the ever-changing risk landscape, internal auditors must keep their skills and expertise current with training and knowledge of industry best practices. This is not easy to do with limited resources.

Third is being relevant in the organization. Many times, internal auditors are not viewed as having the strategic-thinking ability necessary to be included in key management decisions. As such, internal audit is not included in strategic or major initiative discussions, and often it is relegated to a back-office position.

How can small audit functions use their limited staff resources to be more effective?

WATTS The internal audit function needs to work

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

closely with senior management and the audit committee to ensure its mandate is aligned with the organization's strategy and objectives. Small internal audit functions need to think about how others in the organization can help mitigate risk. For example, the internal audit function should spend time educating process and compliance people in risk identification and mitigation to help fortify risk management. This will help alleviate the pressure on the internal audit function being the last and only line of defense. By helping to spread the risk management burden across the organization, internal audit can balance its resources and skills to higher risks and more value-added risk-focused areas.

KASTENSCHMIDT Internal audit needs to work collaboratively within the organization. Audit doesn't need to execute the work for it to be valuable to the risk management objectives of an organization. Rather, it needs to understand the various risk management activities happening within the organization and paint a complete picture for stakeholders of how those various efforts work together to adequately manage and monitor risk.

The small internal audit function also needs to spend sufficient time on the risk assessment to ensure it is auditing the right areas, and then spend considerable time up front defining the scope and approach of the audit, itself. It is far better to have a well-planned audit for which the expectations are clear than to prematurely charge into an area only to discover that success hadn't been defined and thus can't be achieved.

How can small functions use technology cost effectively?

KASTENSCHMIDT Small audit functions should select tools appropriate for the size and skill of the environment and be purposeful in integrating their capabilities into the risk management approach. Consistently maximizing the use of a less powerful tool is far superior to constantly struggling with unneeded functionality of unnecessarily robust technology.

The auditors should not become frustrated midway through the technology journey — becoming proficient in tool usage is time consuming. Too many small audit departments stop short of fully integrating a tool into their delivery approach and thus incur much of the cost but realize little of the sustainable benefit associated with a technology investment. Small internal audit functions should move forward only with those technology initiatives that they are committed to sustainably transforming their approach. Audit functions should stay away from those that have a high likelihood of becoming a hobby versus a mission.

WATTS While automated workpaper solutions and data analysis tools can help improve the efficiency and effectiveness of any size internal audit function, the use of technology should be considered in line with the audit function's goals and plans. Internal auditors need to look for ways to align technology where they lack skills and experience, but without jeopardizing risk management at the organization. Technology cannot do the thinking for internal audit.

What role does communication play in the success of the small audit function?

WATTS Communication to and aligning with all stakeholders is very important. This begins with the organization's vision and strategic objectives and should flow down to each audit professional. This is the way to ensure that even the smallest audit function stays relevant and valued by the organization. The audit function should proactively initiate risk management updates throughout the organization and follow up to ensure all are doing their share in defending against risk.

KASTENSCHMIDT Without a clear understanding of why an audit is being conducted, what was discovered, how those observations could impact the business, and what choices management has to address them, an audit is of limited value. Even if tremendous audit work was conducted, if it doesn't have an impact on its intended audience, it was a failure. Auditors should be among the most refined communicators in the entity.

What are some other best practices small audit functions can reasonably adopt?

KASTENSCHMIDT The internal auditors should actively network with industry peers to learn and apply leading practices more quickly. They should actively network within the organization to raise the profile of internal audit, identify potential subject matter experts to integrate into future audits, and stay abreast of changing risks in the organization that may warrant changes to the existing audit plan.

WATTS Auditors in these small functions should become involved with The IIA. Not only are The Institute's professional standards and practice advisories among many resources offered, local chapter meetings offer a great way to connect with other internal audit professionals and gain valuable education.

In addition, small audit functions should leverage continuous control monitoring, use data analytics, lean on business for experts such as guest auditors, and use business partners to supplement specialization.

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

BY JOHN A. GIANNETTI

IF I ONLY KNEW THEN WHAT I KNOW NOW

A former internal auditor shares what, in hindsight, he would have done differently while in the profession.

The time I spent working in internal audit left an indelible mark on my career. During the 10 years I spent in the profession, I developed a new audit department, helped it grow from a small centralized function to a global activity, traveled to many places, and had the opportunity to meet people from around the world. Unfortunately, I never realized then how narrow internal audit's view of the organization can be or the extent to which information is often filtered before an audit team gets to examine it. Had I only attended meetings that I wasn't invited to, spent more time talking to the individuals actually doing the work, or invested additional resources looking beyond the financial statements, I would have added a lot more value.

Meetings often hold the key to organizational decision-making. Most companies today use Outlook or a similar tool for conference-room booking, where each meeting's focus is identified on a master schedule. I am not suggesting internal auditors sit in on annual reviews, but they can easily locate meetings about processes, or about important new initiatives, and insert themselves. Sometimes the individuals leading those meetings don't have the full picture like internal auditors do.

Obtaining the right information frequently hinges on talking to the right people. In many instances, auditors spend much of their time discussing controls and procedures with management—often comprising seasoned veterans and, in some cases, former auditors. They know the questions internal audit will ask, and they know the answers auditors want to hear. For this reason, internal auditors should also talk to the employees performing the day-to-day tasks. These individuals have direct insight on how processes are working and what could make them more efficient. Auditors should speak to the employees one-on-one, form relationships with them, and let them know that internal audit wants to make their job more efficient for the good of the organization as a whole.

Lastly, auditors should spend more time on activities that don't involve the organization's financial statements. Identifying potential concerns beyond the financial statements is often where practitioners add value that can keep the organization from running afoul of regulators. Especially as organizations grow and expand into new countries or jurisdictions, significant risks can be overlooked, as laws may differ among countries or states. Auditors should take the time to research complexities that similar organizations are facing—simple online searches often reveal valuable information.

Opportunities to add value exist everywhere in organizations, but in many cases internal auditors are too busy trying to complete the present tasks at hand, clear review notes, or write management reports. They need to make time to find those opportunities. Auditors don't need to leave the profession and come to these realizations via hindsight— they can start making changes, and adding value, right now. IA

JOHN A. GIANNETTI, CPA, CGMA, CITP, *is director, Tax Accounting and Reporting, at Health Care REIT Inc. in Toledo, Ohio.*

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

100+
Speakers From Around the Globe

65+
Sessions in 10 Educational Tracks

2,000+
Attendees from 100+ Countries

Mountains of Change... Oceans of Opportunities

Join audit professionals from globally recognized and Fortune 500 organizations at the 74th annual IIA International Conference, July 5–8, 2015, in beautiful Vancouver, BC, Canada.

Confirmed Keynote Speakers

Theresa Payton
Founder, Fortalice, LLC
Former White House Chief Information Officer

Yuwa Hedrick-Wong, Ph.D.
Distinguished Visiting Professor, University of British Columbia
Global Economic Advisor, MasterCard Worldwide

Conference delegates enjoy special discounts on accommodations at convenient downtown Vancouver hotels. Book your accommodations when you register for the conference and receive up to CAD$200 in savings.

Earn up to 18 CPE.
Visit **ic.globaliia.org** to register today!

THE INSTITUTE OF INTERNAL AUDITORS
INTERNATIONAL CONFERENCE
VANCOUVER, BC, CANADA / JULY 5-8, 2015
VANCOUVER2015

2015-5033

2015 TeamMate® User Forum

Experience unique networking opportunities, exciting social events, and content-filled learning sessions that empower auditors and provide audit departments with a technological edge.

September 27-30, San Antonio, Texas

The Early Bird Gets the Worm

Register by May 31 and save 15%

www.TeamMateUserForum.com

Wolters Kluwer
Audit, Risk & Compliance

PRINCIPAL PARTNER