Ia
INTERNAL AUDITOR

DECEMBER 2015

INTERNALAUDITOR.ORG

Fifteen of the profession's best and brightest are emerging as leaders of tomorrow.

ON THE RISE

Whether you’re already using TeamMate or thinking about becoming part of our community, letting us host your audit solution is a great way to improve efficiency, stay current, and eliminate costly IT support wait times.

Call us today at 1-888-830-5559
or Learn more about TeamMate at TeamMateSolutions.com

Wolters Kluwer

IIA PRINCIPAL PARTNER

Ia
INTERNAL AUDITOR

DECEMBER 2015 VOLUME LXXII: VI

FEATURES

Ia

INTERNAL AUDITOR

DECEMBER 2015 VOLUME LXXII: VI

DEPARTMENTS

PRACTICES

INSIGHTS

ONLINE InternalAuditor.org

Leading the Way Learn more about the current crop of up-and-coming audit professionals in our supplement highlighting the honorable mentions from this year's Emerging Leaders.

Slick Dealings Art Stewart discusses what auditors can learn from a forensic audit that discovered an Indonesian energy company's trading unit was paying artificially high prices for oil imports.

CBOK 2015: Challenges for the Public-sector Auditor Watch a video rundown of government-specific findings from The IIA Research Foundation's Global Internal Audit Common Body of Knowledge report.

Auditing the Internet of Things The rise of Internet-connected devices and systems brings both new opportunities and risk for modern organizations.

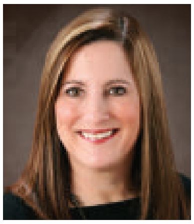
Find us on Facebook

Internal Auditor ISSN 0020-5745 is published in February, April, June, August, October, and December. Yearly subscription rates: $75 in the United States and Canada, and $99 outside North America. No refunds on cancellations. Editorial and advertising office: 247 Maitland Ave., Altamonte Springs, FL 32701-4201, U.S.A.

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.

ILLUSTRATIONS: TOP, MICK WIGGINS / THE I-SPOT.COM
RIGHT, ROBERT KNESCHKE / SHUTTERSTOCK.COM

Editor's Note



LEADERS FOR A LIFETIME

The IIA regularly recognizes internal audit professionals for their contributions to the profession. From the American Hall of Distinguished Audit Practitioners, to awards such as the William G. Bishop Lifetime Achievement Award and Victor Z. Brink Award for Distinguished Service, The Institute acknowledges the achievements of accomplished auditors who have led the way in ensuring that internal auditing is perceived as a necessary and valuable contributor to the organization's growth and well-being.

One has to wonder if these accomplished professionals displayed promise from the start. Did they stand out from their peers? Did their curiosity, dedication, and innovative ideas identify them to their supervisors as emerging internal audit leaders?

For the past three years, *Internal Auditor* has striven to identify and feature rising talent in the profession—those potential future winners of IIA lifetime achievement awards who are already displaying the leadership characteristics that separate them from their peers. In this issue, we celebrate *Internal Auditor's* 2015 Emerging Leaders, which includes some of the best and brightest the profession has to offer. How do we know that? We asked our readers.

Readers from around the world nominated these outstanding individuals based on their professionalism, leadership abilities, thirst for certification, advocacy of the profession, and innovative thinking. These well-rounded individuals also are very active volunteers in their communities. A panel of judges chose from blind nominations those young practitioners who truly represent the future of the profession. A big thank you goes out to this distinguished panel, which includes representatives from The IIA's Global and North American boards, The Institute's Publications Advisory Committee, and past emerging leaders, for helping us choose such an exceptional group.

As you can see, past emerging leaders don't fade away. We keep them busy. The magazine and The IIA are taking advantage of having their fresh perspectives on the profession and work life, in general, to help us understand what is important to the next generation of internal auditors. This month, we are excited to announce the launch of our Emerging Leaders blog. Visit InternalAuditor.org to learn what these professionals, including past Emerging Leaders Seth Peterson, Mike Levy, and Laura Soileau, have to say about the state of the profession and what makes a successful internal auditor today.

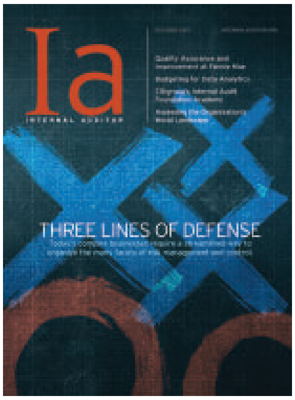
Beginning on page 30, we are proud to introduce to you the class of 2015 *Internal Auditor* Emerging Leaders! Also, visit InternalAuditor.org to view the list of 2015 Emerging Leaders Honorable Mentions. Congratulations to all of these internal auditors who are well on their way to becoming the leaders of tomorrow.

Anne

@AMillage on Twitter

Reader Forum

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



The Three Lines

I object to the premise in "Defense in Depth" that the three lines of defense is something to be "implemented." Rather, it is a communication tool that helps to define the role of risk assurance functions. Recently, while sitting in an audit committee meeting, the chairman asked a great question about redundancy of coverage between internal audit and compliance. In this case I used the three lines of defense to describe their unique roles. However, while the three lines of defense may do a lot to help auditors improve their view of operational management and their ownership of risk, it does not create a model or framework by which to measure governance or management operational risk exposure because of their choices.

DAN CLAYTON *comments on Jane Seago's article, "Defense in Depth" (October 2015).*

Audit Transformation

I really enjoyed Mark Carawan's description of Citigroup's Internal Audit Foundation Academy. The idea of a core curriculum that allows you to disperse staff while ensuring consistency of results is tremendous. Congratulations on what sounds like a resounding success for his audit function!

STEVE SCHOENLY *comments on Mark Carawan's article, "A Strong Foundation" (October 2015).*

Team Motivation

Nnennaya Anyaebosi nicely summarized some of the key factors in retaining talent. In addition to some of the factors she mentioned, I also think it's important for managers to understand what motivates and engages employees. I am part of a small internal assurance team. One of the experienced team members moved into a new role, leaving us understaffed during year-close. My managers and the director handled the situation well. They organized meetings with staff periodically to discuss workloads and progress, and redistributed or reprioritized the work, if needed. Their positive reinforcement and appreciation were helpful, and they understood what would motivate the team to take on this challenge.

RENUKA CHHATRE *comments on Nnennaya Anyaebosi's article, "Are You Driving Away Talent?" ("In My Opinion," August 2015).*

Trusted Advisers

Richard Chambers has (probably unintentionally) raised a good debate about what it means for internal audit to be trusted advisers. I fully understand (and feel) the pressures from the business to extract as much value from internal audit as possible, but as a result, many times the line between the second and third lines of defense becomes more blurred than it should. After all, internal audit's reporting line, from a functional perspective, is

Ia
INTERNAL AUDITOR
DECEMBER 2015
VOLUME LXXII:VI

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")

the board, not management, and our primary job is to provide an opinion about the right balance between risks and controls. That means that the business advisory role comes in second place, our primary mandate being to provide an independent view of risk management effectiveness; more specifically, the quality of the governance and internal control systems.

BRENO GALVAO *comments on the Chambers on the Profession blog post, "From Trusted Adviser to Double Agent: Are Regulators Trying to Redefine Internal Audit?"*

Not My Problem

Norman Marks has a point worth considering, that separate board committees might tempt the rest of the board into complacency by thinking, "The risk committee does risk management, so it's no longer my problem." It's a valid concern.

What strikes me, though, is the simple correlation: If you have a risk committee, your audit committee (and your compensation committee, according to more research I've done) has the word *risk* in its charter more often. To my thinking, if nothing else, that phenomenon pushes other committees to think about risk in a more disciplined fashion—and that alone is worth the effort, because a more disciplined approach to risk management is sorely needed.

MATT KELLY *comments on the Marks on Governance blog post, "How Much Should Audit Committees Worry About Risk?"*

Working Overtime

I agree with Mike Jacka that while there are some jobs, on an assembly line for example, where the quantity produced varies with the time worked, this rule doesn't often apply to "knowledge" workers. Many part-time workers will say they achieve in three days what their full-time co-workers achieve in five days because they have to manage their time.

I know I'm being simplistic and don't want to belittle the work of internal auditors who do work weekends, but in too many instances it's bad time management—usually by the managers.

DAVID GRIFFITHS *comments on the Mind of Jacka blog post, "There Are Never Enough Hours in the Week - Part One."*

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

Update

BOARDS GIVE INTERNAL AUDIT HIGH MARKS

Survey also suggests directors are balancing short-term pressure and long-term shareholder value.

Respondents to the 2015 Corporate Directors Survey from PricewaterhouseCoopers (PwC) give internal audit good grades, with 90 percent of audit committee members reporting that internal audit's skills, leadership, corporate stature, and materials given to the board are good or excellent. Similarly, 90 percent of audit committee members say internal audit's organizational status is good or excellent, and only 8 percent say internal auditors' stature needs to be improved.

Don Keller, a partner in PwC's Center for Board Governance in New York, says audit committees like what they see with internal audit. "Ninety-six percent of them believe internal audit's willingness to stand their ground is good or excellent." But, he adds, "Directors say they have considerably more confidence in the stature of large company internal audit groups than with smaller cap company groups." Sixty-three percent of respondents serve on an audit committee.

The responses from 783 directors of publicly listed companies provide insight into boardroom thinking, from long-term strategic planning to short-term investor expectations, to activist investors. One issue

CERTIFICATION PAYS

Overall, internal auditors with professional designations earned higher median salaries this year.

U.S. MEDIAN
SALARIES

CRMA-US$112,896

CISA-US$105,000

CIA-US$93,150

CPA-US$92,218

CFE-US$92,218

NO CERTIFICATION
US**$65,000**

Source: The IIA Audit Executive Center, 2015 Internal Audit Compensation Study

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

ILLUSTRATIONS: TOP, MICK WIGGINS / THE I-SPOT.COM
RIGHT, PELIKEN / SHUTTERSTOCK.COM

79%

OF TOP EXECUTIVES, RISK PROFESSIONALS, AND BUSINESS CONTINUITY MANAGERS say reputational damage from a sensitive data breach would be the most likely and highest impact risk scenario.

28%

OF CEOS

surveyed say their organization has dedicated insurance coverage against cyberattacks.

6%

OF RISK MANAGERS

say their organization has such coverage.

"CEOs overestimate their levels of protection for the risks they consider to be the most likely and high-impact," according to the 2015 International Business Resiliency Survey.

Source: Marsh and Disaster Recovery Institute International

activist investors and other stakeholders are calling for is greater representation by women and minorities on boards.

However, the report notes women are far more likely to consider board diversity important—63 percent of women say gender diversity is very important compared to 35 percent of men. Racial diversity is considered very important by 46 percent of female directors versus 27 percent of male directors. Seventy-four percent of female directors say they "very much" agree that board diversity leads to enhanced company performance, compared to only 31 percent of males.

Among other key findings, directors are more engaged in IT issues, with 83 percent saying they are at least moderately engaged in comprehending the status of major IT implementations, compared to 77 percent last year. Moreover, 83 percent report they are moderately engaged in cyberattack oversight. More than half of respondents say IT oversight is the responsibility of their board's audit committee. **—S. STEFFEE**

ALARMING RISK ASSESSMENT TREND

A PCAOB report says many external audits don't comply with its risk standards.

U.S. Public Company Accounting Oversight Board (PCAOB) inspectors found deficiencies in more than one-fourth of 2012 and 2013 external audit engagements they examined in which the board's risk assessment standards were applicable. Preliminary data on 2014 inspections show the trend continuing.

Auditing Standards (AS) No. 8 through No. 15 comprise the PCAOB's risk assessment standards. According to a recent report, the most frequently identified risk assessment deficiencies related to AS No. 13, The Auditor's Responses to the Risks of Material Misstatement; AS No. 14, Evaluating Audit Results; and AS No. 15, Audit Evidence.

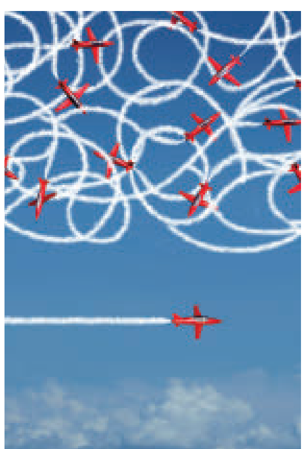
The report says audit firms failed to perform procedures that responded to fraud and other identified risks (AS No. 13), evaluate the accuracy and completeness of financial statement disclosures (AS No. 14), and consider relevant evidence that may have contradicted financial statement assertions (AS No. 14). Firms also did not sufficiently test the design and effectiveness of controls to support their level of control reliance (AS No. 15).

"Because risk assessment underlies the entire audit process, it is critical that audit firms address these findings of weaknesses in compliance with the risk assessment standards," PCAOB Chairman James Doty says. **– T. MCCOLLUM**

DEVICE RISKS UNDER THE RADAR

Cybersecurity professionals say Internet of Things security falls short.

Nearly three-fourths of IT professionals surveyed say the likelihood of their organization experiencing a security breach because of interconnectivity via the Internet of Things (IoT) is medium to high, a recent ISACA report finds. Roughly



the same proportion of respondents says IoT device manufacturers are not equipping their products with adequate security measures.

ISACA's IT Risk/Reward Barometer study depicts an IoT that flies below the radar of many IT organizations, resulting in an

PHOTO: LEFT, LIGHTSPRING / SHUTTERSTOCK.COM

MORE Visit InternalAuditor.org to read an extended interview with Kenneth Metz.

"invisible" risk that respondents say is underestimated and undersecured. Half of the 2,000 U.S.-based IT and cybersecurity professionals who were surveyed, for example, say their IT department is not fully aware of the organization's connected devices, including thermostats, fire alarms, and even cars. Moreover, 73 percent report that current security standards do not address the risk that IoT poses and say that IT departments need updates or new standards.

The study also highlights a lack of consumer awareness concerning the vulnerabilities posed by interconnected devices and the countless potential entry points they provide for cyberattackers. Sixty-four percent of U.S. consumers, according to the research, are confident they can control IoT security on the devices they own, yet only 20 percent of security professionals share their optimism. Privacy represents a concern, too—88 percent of IT pros say device makers don't make consumers sufficiently aware of the type of information IoT devices can collect.

"Device manufacturers should lead the charge in adopting an industry-wide security standard that addresses IoT security, and put in place rigorous security governance and professional development for their cybersecurity employees," says Robert Clyde, ISACA's international vice president. **— D. SALIERNO**

MAKE THE COMPANY BETTER

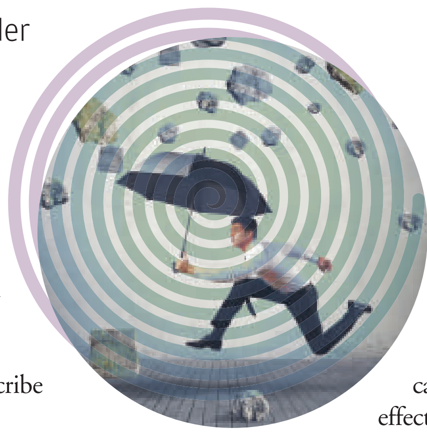
Diverse backgrounds and a collaborative approach enable Xerox CAE Kenneth Metz's internal audit department to provide enhanced insight to the business.

What is internal audit's role at Xerox?
Internal audit's role is to make Xerox better. Using a collaborative approach focused on improvements has been well-received by the business. Because we have a separate internal control function that handles Sarbanes-Oxley testing, internal audit can focus on other areas. We have a continuously expanding role to tackle different types of financial, control, operational, IT, governance, and compliance projects.

What skills do you look for when staffing Xerox's internal audit department?
The key things I look for are a collaborative mentality, good critical thinking skills, strong interpersonal skills, solid writing skills, and subject matter expertise. A positive attitude and a desire to travel to different locations are always helpful. The department currently has a mix of diverse backgrounds with concentrations in auditing, internal control, and IT. Recently, our focus is bringing in people with more IT, analytics, and health-care experience. Professional credentials are also important.

BANKS REASSESS RISK CULTURE

Reforms are part of a broader effort to enhance risk systems and processes.



Bank management and boards around the globe are reforming their risk culture, according to a recent EY survey of financial institutions. Rethinking Risk Management finds that three-fourths of respondents are making changes to their culture, although 81 percent describe that change as a work in progress.

Banks are approaching cultural reform by strengthening risk governance, clarifying what constitutes "acceptable risk," better aligning incentives with risk objectives, and determining how best to handle rule breaches, according to the report. Nearly all respondents, in fact, say severe breaches of the firm's risk policies result in disciplinary actions. Many also point to the importance of communication, with nearly half blaming risk culture breakdowns on failure to cascade messages effectively throughout the organization.

The firms' attention to culture falls within a broader reassessment of risk management practices, according to the report. Banks are moving steadily to enhance risk management systems and processes to meet regulatory and market demands for better controls, and to help prevent future financial crises. **— D. SALIERNO**

PHOTO: RIGHT, ALPHASPIRIT / SHUTTERSTOCK.COM

BY ÖZGE AŞÇIOĞLU + M. TAHA EROĞLU + AYÇA ÜLKER EDITED BY JAMES ROTH + LAURA SOILEAU

THE EFFECTIVE AUDIT REPORT

A well-written report can get stakeholders' attention while raising awareness of internal audit's work.

It is always possible to write a better audit report. Needless to say, many reports do not fulfill their purpose. Although deadlines, piecing work together, and maintaining user readability are stress factors, writing a report doesn't have to be a daunting task.

Knowing the requirements and expectations of the target audience is the first step toward writing a better audit report. Content should be easy to read and provide information to keep the stakeholders' attention. Several suggestions can help ensure stakeholders read the report and go further into detail.

Include employees in the reporting process. Organize solution-design meetings, exchange ideas, and get employees' opinions on action plans, because they are the ones who take the corrective actions related to the findings. Related process owners can suggest different solutions that will help achieve company objectives and have a positive impact on stakeholders.

Determine the target audience. Who is the report presented to and what kind of business habits do they have? Reports have different audiences—clients, senior management, the audit committee, and regulators—with different concerns and focus points. In short, make sure the report meets the expectations of all stakeholders.

Be sensitive to time constraints. Audit clients have numerous duties and responsibilities, and hectic schedules. They want to read about subjects that are important to them and not have their time wasted.

Thank the client. Even if there are no positive findings to report, do not forget to thank clients for helping during the audit fieldwork. This goes a long way to help build business partnerships and maintain long-term relationships with audit clients.

Keep reports simple. State strong points—such as well-designed control processes, outstanding results and achievements, or best practices—in the process being audited. Sentences should be concise, simple, and comprehensible. Long, redundant sentences and repeating what has already been said several different ways does the reader no good. Use shorter paragraphs and subheadings to separate sections. Clients can call if they need more detailed information.

Be careful with executive summary content. The executive summary should provide an overall picture of the findings and action plans. Keep the details of the work to the main body of the report; don't suffocate executive summary readers with excessive details, numbers, and data. Just show the

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

TO COMMENT on this article,
EMAIL the authors at ozge.ascioglu@theiia.org

big picture. If it's all given away in the summary, no one will read the rest of the report.

Enlist a report mentor. After completing the first draft, share it with a colleague and get his or her opinion. Feedback can help reduce the number of revisions, and the reviewer's experience can be used to the auditor's advantage.

Report Ownership

Though it is the final product of an internal audit, the owner of the report is the client. Instead of using traditional audit reporting processes—which consist of findings, recommendations, management response, and final internal audit opinion steps—schedule meetings with process owners first and then mid-management about the findings and action plan as auditors discover them. Determine an agreed management action, which means action is decided concurrently by both auditor and client. Solution-design meetings include management level in the reporting process, which facilitates report ownership and actions and also helps to simplify reporting. As a result, the C-level is able to see the big picture.

Increase Awareness

Auditors may have written a "perfect" report that explains all critical risks and recommended mitigating actions, but all of this means nothing unless it is presented to the right people at the right time and communicated appropriately. The key methods to communicate effectively and emphasize value added are determining the distribution list, submitting the report via email and delivering a hard copy, and making a short presentation or holding a closing meeting with key stakeholders to highlight critical issues. Internal auditors miss the opportunity to elevate the level of importance of their work when the work is not completed accurately. They also may miss the opportunity to increase awareness levels of internal audit and internal control within their organization. Ia

ÖZGE AŞÇIOĞLU, CIA, CFSA, CRMA, CFE, *is CAE at Avea in Istanbul.*

M. TAHA EROĞLU, CCSA, CRMA, *is an internal audit manager at Avea.*

AYÇA ÜLKER *is a senior internal auditor at Avea.*

BY LANCE J. SEMER EDITED BY STEVE MAR

MEDICAL DEVICE CYBERSECURITY

Internal auditors can help health-care providers ensure their devices benefit patients – not threaten them.

Securing computer systems is common practice, but the same cannot be said for off-the-shelf (OTS) medical devices containing embedded computer systems, which are vulnerable to threats that could expose patients to harm. For example, attackers could exploit flaws in wireless-enabled medical implants to trick an insulin pump into delivering a lethal dose or reset a pacemaker to deliver a fatal shock.

Concerns over such attacks prompted former U.S. Vice President Dick Cheney's doctors to disable the wireless functionality of his pacemaker in 2013. The potential threat from criminal organizations, hostile nations, and others is so great that the U.S. Department of Homeland Security is working with the U.S. Food and Drug Administration (FDA), medical device manufacturers, and health-care professionals to address device vulnerabilities.

In addition to threatening patients' health, compromised medical devices connected to health-care provider networks may enable hackers to steal patient data, resulting in the unauthorized disclosure of personal health information (PHI). According to Reuters, medical information is worth 10 times more than customer credit card numbers on the black market because it can be used to create fake IDs to buy medical equipment or drugs, as well as to file fraudulent insurance claims. Based on these safety and data security concerns, internal auditors who work in the health-care industry or for benefit providers need to be aware of medical device risks and ensure their organizations have effective mitigation programs in place.

Governmental and Industry Concerns

In 2012, the FDA released Strengthening Our National System for Medical Device Postmarket Surveillance, which advocated several key objectives:

- Establish a multi-stakeholder planning board to identify the governance structure, practices, policies, procedures, and business models necessary to facilitate the creation of an integrated medical device post-market surveillance system.
- Establish a unique device identification (UDI) system and promote its incorporation into electronic health information.
- Develop national and international device registries for selected products.
- Modernize adverse event reporting and analysis.
- Develop and use new methods for evidence generation, synthesis, and appraisal.

The FDA's October 2014 guidance for the medical

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

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

device industry, Content of Premarket Submissions for Management of Cybersecurity in Medical Devices, encouraged manufacturers to consider cybersecurity risks throughout the development and manufacturing cycle. In addition to the FDA, the Institute of Electrical and Electronics Engineers (IEEE) released Building Code for Medical Device Software Security to help manufacturers mitigate cybersecurity weaknesses.

Collectively, these guidelines are not easily enforceable, can be difficult to implement, and may not be legally binding. As such, health-care providers that rely on these devices for patient care and services should exercise their own due diligence to ensure they are safe, reliable, and secure.

Risk Factors

To understand what needs to be protected, internal auditors must first become familiar with the FDA and IEEE guidelines and other health-care industry sources. OTS medical device areas that should be scrutinized by internal audit include:

- *Operating systems.* Many medical devices still run on old, unsupported operating systems that are vulnerable to hacking exploits and UNIX variants with unsecure default configuration settings.
- *Security patching.* Unlike conventional network components, medical devices typically cannot accept security patch updates because they rely on closed operating systems that can only be updated by the manufacturer.
- *Application software.* IT teams usually cannot access medical device internal software to ensure cybersecurity safeguards are in place and operating effectively.
- *Antivirus and antispyware.* The ability to install and update antivirus and antispyware capabilities within medical devices is typically restricted to the manufacturer.
- *Passwords.* Device passwords most often are not changed when installed and remain set at the manufacturer's default value, which easily can be guessed or obtained from user manuals and other sources on the Internet.
- *Wi-Fi and Internet connectivity.* Home-use therapeutic and monitoring devices with Wi-Fi and Internet cloud connectivity allow the patient's health-care team to monitor medical information in real time, as well as change settings remotely, if needed. Although convenient, threat actors can exploit compromised devices to hijack connections, steal patient information, and alter device settings that could threaten the patient's well-being.

Internal auditors should determine whether their organization has an OTS medical device risk mitigation program in place that includes:

- Documented policies and procedures to manage and secure medical devices.
- Processes to maintain an up-to-date inventory of medical devices with UDI tracking capabilities.
- Routine security risk assessments using defined metrics to identify which devices are at high risk and require remediation, replacement, or to be placed out of service.
- A vendor management program that coordinates with device manufacturers to address security updates for embedded applications, operating systems, software patches, and anti-malware.
- Stakeholder partnership with the Medical Device Postmarket Surveillance System Planning Board.
- Organizational collaboration with manufacturers and security experts to identify device security gaps, vulnerabilities, and remediation solutions.
- Procedures to ensure that medical device default passwords are replaced with complex passwords that are changed frequently.
- Disabling device Wi-Fi and Internet connectivity, if it is not required.

Additional Considerations

Aside from securing OTS medical devices themselves, health-care providers should invest significantly in a robust, hardened IT infrastructure supported by multilayered security solutions to detect and defend their networks against cyberattacks that exploit compromised medical devices. Data loss prevention solutions also should be in place to mitigate risks associated with the theft of PHI.

A health-care provider's ability to remove high-risk, network-connected devices and disable patient-owned equipment may not be feasible because such measures might disrupt patient care and services and be too costly. Accordingly, providers may be forced to accept risks associated with vulnerable devices until viable solutions can be implemented. Providers faced with this dilemma should reassess their risks and revisit their insurance coverage to ensure they address damages caused by compromised medical devices. Organizations also should ensure that their incident response teams and public relations departments have plans in place to effectively respond to incidents stemming from compromised medical devices.

Health-care providers that overlook or ignore the pervasive cybersecurity threats associated with OTS medical devices may face elevated legal, regulatory, and reputation risks. To ensure compliance with legal and regulatory requirements, internal audit at these organizations should advise management about these concerns in addition to including reviews of these devices in their audit plan. Ia

LANCE J. SEMER, CIA, CISA, CISSP, *is the information security officer for Washington Federal in Seattle.*

BY RICHARD J. MACHOLD EDITED BY PAUL SOBEL

THE FOUR HATS OF RISK MANAGEMENT

Internal auditors can assess ERM's impact through the lens of architects, facilitators, aggregators, and communicators.

Enterprise risk management (ERM) practitioners know that the discipline has a tendency to create an extensive and sometimes overwhelming array of elements, including framework, policy, process, dashboards, and tools. All of these are good and necessary means to an important end. However, as internal auditors increasingly are being called on to provide meaningful assurance over ERM, their approach often is to ascertain whether these elements (the means) are present and functioning without full consideration of ERM's ultimate impact and value (the end). In other words, internal auditors can conclude that all the elements exist, but how do they know that ERM is truly making a positive and enduring difference in the business?

IIA Standard 2120: Risk Management instructs internal auditors to adopt a holistic assessment lens that spans multiple engagements across which issues are viewed together. This implies a higher level construct for ERM assessment that requires internal auditors to transcend the typical audit program and look at ERM through the lens of fundamental organizational capabilities. All these capabilities must be active to ensure ERM has its desired impact. Just as the author and consultant Edward de Bono's Six Thinking Hats system separated thinking into distinct functions and roles, a "Four Hats" approach to risk assessments directs internal auditors to look for how key organizational strengths and capabilities are applied, as well as their resulting impact on the business and its culture.

Hat 1: Architect/Builder

ERM is a one-size-fits-*one* proposition for organizations. Therefore, striking the optimal design and positioning of ERM for a specific organization is essential. It goes beyond determining how many risk committees the organization should have; which governance, risk, and control tool it should use; and whether it should use a three- or a five-point rating scale.

The architect/builder should look across the three lines of defense to see how risk is currently being owned and managed and whether any line of defense might be overly dominant or inappropriately weak. For example, does the second line "over-function" with respect to certain risks such as compliance and data security, thereby allowing the first line to abdicate its ownership responsibility to the second line? Or worse, do the first and second lines look inappropriately to the third line for primary risk and control ownership? This hat also considers the organization's appetite and capability for change, anticipates points of resistance, and incorporates

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

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

a results-focused and driven organizational change strategy into ERM's development and execution.

Internal audit should look for: The central ERM team should have a master-plan mind-set and capability that continuously drives purposeful and flexible ERM design and operation, and leverages and tailors existing management practices before creating new, separate ones. Internal auditors should look for evidence that substance outweighs form in the ERM process and that periodic monitoring leads the way to necessary course corrections when the program shows signs of stress.

Hat 2: Facilitator/Coach

In a truly productive ERM process, risk thinking and action are continuously being embedded into the fabric of the business. Some individual or group must take the lead in equipping the organization's people to move toward second-nature risk thinking about: 1) What are we trying to achieve? 2) What and how big are the opportunities and obstacles? and 3) How do we best respond?

The facilitator/coach recognizes there is an indispensable equipping role for the central ERM team. The team must replicate its skills, knowledge, and practices throughout the organization over time to truly build a healthy risk-managing business. Therefore, the chief risk officer and the ERM team's principal players have an evangelistic aspect to their mission that requires them to garner a high level of professional respect and credibility. Absent the right amount of credibility, the ERM leader will inevitably struggle as a minority proponent among a skeptical majority.

ERM must tell the "big picture" about the organization's risk profile.

Internal audit should look for: Auditors should determine whether the central ERM leader and team passionately and purposefully teach ERM knowledge and skills to personnel throughout the organization. They should look for evidence that a growing risk mind-set is active across all three lines of defense, not just in the risk committee meetings. Also, they should seek out and highlight anecdotal examples of beneficial ERM application, and look for indications that risk and control ownership resides where it belongs within the three lines.

Hat 3: Systems Thinker/Aggregator

ERM tends to produce volumes of data that stop short of providing real knowledge and decision-supporting insight. To provide genuine risk insight and not just raw information, the ERM process must be capable of telling the "big picture" story about the organization's risk profile.

The systems thinker/aggregator strives to connect the dots across risk registers, heat maps, and bubble charts, and develop the higher-level insights and conclusions that inform risk decisions. For example, instead of just presenting a one-dimensional top 10 list of risks, the systems thinker might ask which of the risks in the list are the driving/causal risks (events, conditions) in the system, and which are the more passive/reactive (effects, consequences) risks. The aggregator might then ask how certain risks relate to one another and attempt to find cross-cutting themes about the overall risk profile.

Internal audit should look for: Auditors should look for evidence that the ERM team is doing the hard work of discerning and delivering the deeper, higher-level risk insight that otherwise might not be obvious.

Hat 4: Communicator/Influencer

The ERM leader and team must be able to communicate compellingly and clearly to inform major risk decisions. The value is in the dialogue—the purposeful interactions ERM fosters among risk-taking decision-makers. The best risk analysis will be of little use without a compelling and clear message that communicates real life implications to the business. Like the facilitator/coach, the ERM leader wearing the communicator/influencer hat and his or her team must be truly respected and deemed credible on a peer-to-peer level with executive and senior management.

Internal audit should look for: The ERM team should demonstrate excellence in communicating with influence and have a high degree of organizational stature. Auditors should look for evidence that the output from the ERM process is clear and compelling, and that a healthy challenge process occurs regularly within the risk dialogue.

More Than the Sum of Its Parts

Good and thorough guidance abounds for assessing ERM programs according to traditional frameworks and established best practices. In addition to such practices, internal auditors should continually challenge themselves to evaluate ERM programs according to the organizational value they provide over time. By assessing the ERM program using the Four Hats approach, internal audit can determine whether the initiative has graduated beyond having the necessary parts to truly make a positive difference for the organization overall. Ia

RICHARD J. MACHOLD, CIA, CPA, CRMA, *is CAE of Total System Services Inc. in Columbus, Ga.*

BY DANNY COSTON EDITED BY JOHN HALL

WHO'S KEEPING YOUR BOOKS?

A bookkeeper in charge of daily bank deposits pockets nearly US$50,000 from her unquestioning employer.

Phil Stewart owned a heating, ventilation, and air conditioning business that employed 286 people. He trusted his employees and, unfortunately, did not feel the need to put controls in place. As a result, Stewart became a victim of embezzlement by a trusted employee.

Because of the lack of segregation of duties in the company's accounting department, a tax consultant suggested to Stewart that the company evaluate its accounting and financial internal control procedures. This meant a complete review of all the policies and procedures designed to protect the company's assets and financial information.

Stewart was adamant that an internal control review would be a waste of the company's time and money. His bookkeeper, Shirley Thompson, had been faithfully taking care of the company's accounting duties for many years. Because he trusted her, he also had her doing his personal accounting and banking. However, after some persuasion, he decided to move forward with the review.

What the auditor found was that Thompson had stolen nearly US$50,000 from the company over five years. The fraud was easy to commit because her duties included preparing the daily bank deposit slips, making deposits at the bank, and preparing the monthly bank reconciliations. She would take between US$100 and US$500—sometimes more—from the daily bank deposits and cover the shortages by adjusting journal entries to various accounts in the accounts receivable ledger. No one reviewed Thompson's work or questioned her recordkeeping.

The company's receptionist, Sally Newberry, would open up the mail each day and list the received check payments on a daily log of cash receipts. Newberry would then make two photocopies of the daily cash receipts log and give one copy to Thompson and one to the office manager. There were obvious problems with this cash control procedure. Newberry filed her copy of the daily cash receipts log in her cabinet and never compared the list with any bank deposit slips or the deposits on a bank statement. In addition, the office manager filed his copy and never compared it with any bank deposit slips or the deposits on the bank statement. Thompson, too, filed her copy away and never looked at it again. In addition, no one reviewed the bank reconciliations prepared by Thompson, nor was there a review of the activity in the ledger.

Stewart was devastated to learn what Thompson had been doing. He terminated her but decided not to press charges when he found out why she was taking the money. Thompson was a

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

TO COMMENT on this article, **EMAIL** the author at danny.coston@theiia.org

single parent with a young daughter who was ill and in need of medical attention. Even with the company's insurance plan, she could not afford to pay for her medical costs.

Lessons Learned

- A strong system of internal control is key for any business owner to avoid a situation like this. The purpose of internal controls is to foster reliable financial reporting, safeguard assets, and promote ethical conduct. For example, controls must exist over the maintenance of vendor lists, and user access to the accounting systems must be monitored and restricted by the use of passwords and user activity logs.
- Ensuring segregation of duties in the cash receipts and cash disbursements area is a critical internal control that no organization should overlook. For example, a small-business owner should ensure that the requisition, approval, and processing of all cash disbursement transactions are not performed by the same individual.
- A cashier should open remittances in the presence of a responsible employee and immediately endorse checks with a stamp stating, "For Deposit Only." Cash and checks should be kept in a locked and secure area until they can be deposited. Furthermore, the use of budgeting is not only a great planning tool for measuring actual results with forecasts, but unusual variances in business activity also provide a red flag that may require a follow-up inquiry.
- Establishing a company culture with an effective control environment is also an effective tool that a small-business owner should use to deter fraudulent activity, as the mere suggestion of a future investigation can reduce the occurrence of fraudulent behavior among employees. While time may not always permit a 100 percent review of all recorded transactions and related supporting documentation, the business owner should project his or her active oversight of the bookkeeping process by regularly requesting copies of the cash disbursement journals or of all checks and bank reconciliations.

DANNY COSTON, CIA, *is a senior internal auditor at HOYA Vision Care in Lewisville, Texas.*

Meet *Internal Auditor*'s 2015 Emerging Leaders—they're bright, ambitious, and eager to advance the profession.

If this year's Emerging Leaders represent the future of internal audit, then the future of internal audit isn't just bright, it's a supernova. The 15 professionals profiled here—representing five countries and nine industries—are well-educated, and many are pursuing advanced degrees and already hold professional certifications. They're excited by internal audit's evolving position as trusted adviser on just about every endeavor an enterprise undertakes, and they have little patience for its old-fashioned reputation as the "Department of No."

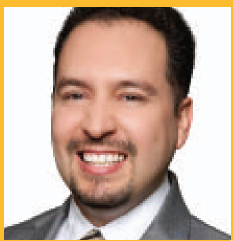
ON THE R

They're much, much more than just internal auditors, getting involved in their communities and taking leadership roles in their local IIA chapters and institutes. *Internal Auditor* congratulates these outstanding practitioners—a distinguished group that will undoubtedly have a positive impact on the profession.

ISE

Russell Jackson

"The best aspect of internal auditing is that it is constantly changing."



Jesus Valdez
CIA

AUDITOR II
SOUTHWEST GAS CORP.

JESUS VALDEZ embraces change. "The best aspect of internal auditing is that it is constantly changing," the 29-year-old University of Nevada, Las Vegas graduate says, adding that he enjoys working on multiple audits at a time and the challenge that comes from juggling priorities. "It's amazing how agile one has to be to adapt to change and still provide valuable information on challenging topics," he says. One additional change Valdez would like to see concerns the negative perception of internal auditors. "Regardless of how pleasant or capable an auditor may be, clients often perceive us as the bad guys, thinking, 'They are only out to get me.' That's outdated and must change." He expects the next decade to be a busy one and has specific career goals in place—five years from now, he wants to become a manager, and in 10 years he plans to be a director. "Ultimately, I want to serve as vice president of the company," he says. Valdez appears well-positioned to achieve those goals. His department is aggressively rebranding its functions to emphasize consulting engagements using analytics software, and he's been instrumental in advocating those services, helping to generate consulting and data analysis requests. The Las Vegas-based practitioner, who has almost five years of internal and external audit experience, is also working toward a master's degree in accounting, the Certified Public Accountant designation, and the Certification in Risk Management Assurance. His past experiences as a student bode well: When he was 14, he was in the top 1 percent of his class statewide and earned a full-ride scholarship to Universidad Autonoma de Chapingo in Mexico. Six months after being admitted, he moved to Las Vegas with his parents—where he learned English as a second language by the age of 15.

Twenty-nine-year-old **CATE NEELEY** has this to share about the profession: "If I could change anything about internal audit, it would be to have a more deliberate approach to marketing how the internal audit activity provides value to the organization through consulting and advisory services." She cites consulting's significant benefits to the organization and its ability to help internal audit promote change, though she adds that management "is often unaware that internal audit has the skill set and availability to provide these services." The diehard Jayhawks basketball and volleyball fan—and MBA holder from the University of Kansas—was recruited as a college junior for a summer internship at Sprint, then was hired and promoted twice in the organization's corporate audit department. She later made a professional move back to the Lawrence-based university. Her boss there, CAE John Curran, says "a combination of great timing and luck allowed me to snag her for our audit manager position." Neeley's ties to her undergraduate alma mater, Pittsburg State University, remain strong as well. She and her supervisor traveled to the university to speak to its students in The IIA's Internal Auditing Educational Partnership; her boss says it was "special to see how she related her experiences in internal audit to a group of undergraduates soon to be starting their respective careers in the profession." Neeley advised them to make effective use of their professional networks, including taking advantage of opportunities provided by the local IIA chapter. She plans to stay in the Kansas City area, she says, and in internal audit as the CAE at, perhaps, the University of Kansas—where she developed the first-ever dedicated internal audit resources at its academic medical center and affiliated research foundation—or at another higher education institution.

ASSISTANT DIRECTOR & INTERNAL AUDIT MANAGER
UNIVERSITY OF KANSAS

Cate Neeley
CIA

"If I could change anything about internal audit, it would be to have a more deliberate approach to marketing [the activity's] value."

15 MAKING A DIFFERENCE

Justin Bonk
CIA, CFE, CISA

"To be successful, we really need to have an extensive understanding of the organization."

MANAGER—ENTERPRISE RISK MANAGEMENT
FREED MAXICK CPAs P.C.

JUSTIN BONK likes to accentuate the positive. If he could change one thing about internal audit, it would be the misperception that internal audit's focus is on the negative aspects of an organization. "That misperception can drive an irrational fear of internal audit," the 29-year-old State University of New York at Buffalo graduate says, "which ultimately creates barriers to communication and hampers our ability to be effective." He acknowledges that much of what internal auditors do involves risk—which often has a negative connotation—but emphasizes that internal audit's true focus is on adding value to the organization by addressing the risk, which he points to as inherently positive. Bringing that positive focus about requires knowledge beyond the walls of the internal audit department. "To be successful, we really need to have an extensive understanding of the organization," Bonk says. "It's satisfying to me, both professionally and personally, to be able to look back after an assignment and think, 'Wow, I have been able to learn so much from this experience.'" He teaches, too, by creating templates and procedures to track and optimize staff test work on audit engagements, providing valuable data to managers for budgeting—and to staff for performance measurement. Currently based in Buffalo, Bonk received a degree in internal audit—somewhat of a rarity in terms of degree offerings, he says—and adds that he knew he wanted to pursue an accounting-related field. After doing some research, he says, internal audit "seemed much more interesting than the other options." He says now he's fortunate to be with a firm that he loves working for and to be part of a team he enjoys working with.

"Internal audit needs more ... unwavering buy-in from senior management."

AUDITOR
FEDEX

Jason Ryu
CIA

Successful career journeys don't always have an auspicious start. "Quite candidly, I didn't know anything about internal auditing before coming into the role," **JASON RYU** says. He vividly remembers the first interview question for the job: Tell us what you know about internal auditing. "I answered honestly that I only had the Google definition I researched the night before," he says, "but that if they were willing to teach me, I would work harder than anyone else to learn." They were, and he did. Now, the 26-year-old Mississippi State University graduate, who's studying for the Certified Fraud Examiner designation, says the most rewarding aspect of his job is the real, tangible changes that derive from auditors' work. But internal audit has to position itself to create value, not react to expectations, he explains. "First, internal audit needs more unprecedented and unwavering buy-in from senior management," he says; second, it should focus on continuous and objective risk management through investment in data analytics. The "greatest irony" in internal audit, he adds, lies in the simple truth that "while we are the catalyst for change, sometimes we are afraid of the very principle that we stand for." He also embraces personal change, noting that he plans for the short term to prepare for the long term. "I'd like to get my MBA and a couple more professional certifications, and also continue improving my Spanish because I'd like to work abroad for a little while," he explains. "My passion has always been traveling and experiencing new places and cultures, so if I can do that and get paid at the same time, obviously that would be a win-win situation."

Justin Pawlowski

CIA, CMA, CRMA,
SAP CERTIFIED APPLICATION ASSOCIATE

"I am challenging manual proceedings from the past ... and coming up with new ideas."

MANAGER, AUDIT—GOVERNANCE & ASSURANCE SERVICES
KPMG AG WPG

JUSTIN PAWLOWSKI wants to change peoples' mind-set about the use of data analytics in internal audit. There's a myth that data analytics is only the task of IT auditors, the 29-year-old with six years of internal audit experience explains, adding, "It's not!" Another misconception is that data analytics may violate data protection laws. "They don't if done right," he stresses. Myth No. 3 is that only internal audit functions with a highly sophisticated tool can apply data analytics successfully. He's emphatic about this one: "That isn't true. Start small, grow big! Keep focused and risk-oriented." Indeed, Pawlowski says he's working to illustrate the great potential data analytics has in internal audit if applied correctly. "When it comes to the use of data analytics in internal auditing, I am challenging manual proceedings from the past and suggesting adapting the internal audit approach and coming up with new ideas and going new ways," says the Frankfurt-based Berlin School of Economics and Law, Anglia Ruskin University, and Goethe Business School graduate. He's specified data analytics-driven testing procedures "for various cash-relevant and process efficiency and streamlining issues, being able to demonstrate quantitative value-add." When he's not revolutionizing the way his company performs internal audit work, he likes to be active—and mobile. He's worked in 15 different countries, and in the last year alone he has collaborated with colleagues from 30 countries for clients around the world. While globe-trotting, Pawlowski likes to indulge his affinity for running—in fact, he never leaves home without his athletic shoes.

"There is something very exciting about coming to a new process and getting to figure it out ... puzzle piece by puzzle piece."

INTERNAL AUDITOR
PORTLAND GENERAL ELECTRIC

Valentina Kostenyuk

CIA, CPA

A couple of college courses started **VALENTINA KOSTENYUK** on her path to internal audit. "I studied accounting and finance at Portland State University and graduated with a dual major in 2011," the 26-year-old explains. "I developed an interest in auditing after taking two audit courses that were very interesting and insightful, and really highlighted the uniqueness of this profession and all the various skills and types of roles it includes." The next step: An accounting internship at Intel made her curious about corporations, so the day after graduation she started as an intern at her current company. "It was a great introduction, and after a few months I was sold on the field," Kostenyuk says. She transitioned into an auditor role and got involved with The IIA's Portland Chapter, where she now serves as president. If she had her way, internal audit would change to a more encompassing and strategic mind-set. "The significant shift toward risk-based audit plans has already occurred," she says, "but that shift should further infiltrate into the design of audit programs, including audit steps and all other activities." That would create greater value for stakeholders at every level, she says, by better aligning the function and activities of internal audit to the organization's overall strategic objectives and risks. But for now, she thrives on the challenge of solving problems. "There is something very exciting about coming to a new process and getting to figure it out, section by section, puzzle piece by puzzle piece," she says. "And realizing how much you learned from both the process and the new people you got to work with is exciting and inspiring."

"My career plan is simple: Learn as much as I can and learn from all who will teach me."

Krystle Pond

AUDITOR II
SOUTHWEST AIRLINES

Not many internal auditors can make this claim: "I have danced in the Macy's Thanksgiving Day Parade in New York City." But **KRYSTLE POND**, 27, can. "It was a fun experience, and I loved every minute of it," she says, adding that she now serves as one of the leaders of the Southwest Airlines Flight Brigade — meaning she gets to march in parades that Southwest Airlines sponsors, including the Magnificent Mile Lights Festival, held in Chicago. She would also like to see the audit profession march forward, hoping to one day see the development of a framework for strategically aligning the internal audit plan with the organization's business initiatives. "Internal auditors are unique in the fact that they touch every facet of an organization, from the front lines to the boardroom," the CIA candidate explains. "Having a documented, systematic approach for aligning internal audit and business objectives will help internal audit focus on management's key risks and concerns, leading to realistic recommendations and action plans given the priorities of the business." Her enthusiasm for the intricacies of internal audit goes back to her college days. While at the University of North Texas (UNT), she began an organization for students interested in internal audit, IT audit, and fraud examination that became UNT's formal student organization for The IIA, ISACA, and the Association of Certified Fraud Examiners. Looking forward, the Dallas-based practitioner sees herself "teaching, coaching, serving, and mentoring future leaders who will contribute to their organizations' success." She adds: "My career plan is simple: Learn as much as I can and learn from all who will teach me."

MARBELIO VILLATORO is passionate about soccer and about family. "I come from a very large family," the 29-year-old California State University, Long Beach graduate says, "and I am part of a competitive soccer team in Long Beach" — one that includes three of his five brothers. Villatoro is also passionate about serving his community. He's been recognized as a community leader by U.S. Rep. Henry Waxman (D-Calif.), Los Angeles Mayor Antonio Villaraigosa, and U.S. Sen. Barbara Boxer (D-Calif.), and has been cited by Raytheon for his Employee Resource Group efforts with the UCLA Philipino Alumni Association. He's also passionate about the interconnectivity of physically far-flung internal auditors. "The global implications that technology, economies, and regulatory requirements have on our stakeholders are creating a greater amount of uncertainty when managing global risks and opportunities," he says. "By leveraging our global resources, training and tools, and our ability to predict future business risks and opportunities, we can evolve our internal audit organizations into global change agents." For now, he strives to perform the function in its finest form. He was asked to lead a complex project at Raytheon that required analyzing roughly 10,000 documents and conducting multiple interviews in a short time. He used text and data analytics to synthesize the plethora of artifacts and leveraged his audit techniques to ensure objective and sound evidence was being formulated. He then used that analysis to communicate that a significant amount of future revenue was at risk — and simultaneously saved the client nearly 500 man-hours by employing these techniques.

INTEGRATED PROJECT MANAGER
RAYTHEON CO.

Marbelio Villatoro
CIA

"By leveraging our global resources ... we can evolve our internal audit organization into global change agents."

ON THE RISE

"What is most rewarding about internal audit is the community we are building together."

James Go

BUSINESS ANALYST, RISK MANAGEMENT
A HUNDRED ANSWERS INC.

JAMES GO wants immersion in internal audit to start much sooner. "I find that young professionals are often unaware of internal audit as a career possibility," the Ottawa, Ontario-based 27-year-old explains. "For those who are aware, it is sometimes difficult to relate to, since it is not rooted in any one academic degree, program, or faculty." If he could, the University of Ottawa graduate, who's pursuing the Certified Internal Auditor and Certified Information Systems Auditor designations, would raise awareness by "establishing more campus-run clubs championed by students and strengthen the role played by academic institutions in preparing students for internal audit opportunities." Toward that end, in fall 2012 he founded the Academy of Internal Auditors Student Club—the plan is to extend its membership base to other universities in Canada. He also says he believes strongly in The IIA as an advocate and educational resource for the profession. "What is most rewarding about internal audit is the community we are building together," he says. "I have seen firsthand the transformation taking place, as the number of interested students from universities and colleges is steadily increasing due to the care and willingness of The IIA to invest where it matters." He serves as chair of academic relations for his local IIA chapter, and he cites five important role models: Kevin Page, the first Canadian Parliamentary Budget Officer; David Coderre, a retired civil servant who now heads his own consulting firm and teaches at the university level; Patrice Aubriot, an audit principal; and Sarah Lyons and Hash Qureshi, principals at his current firm. "They have collectively taught me three fundamental pillars that I follow to this very day," he says, "to vision and pursue, to commit and be passionate, and to care for the changes you want." Moving forward, he plans to mentor others and says he would like to reach out beyond the profession to help nonauditors better understand what internal auditors do. "I hope to share knowledge with other inspirational leaders and transfer their knowledge to create more great leaders."

Jad Antanios
CIA

HEAD OF INTERNAL AUDIT

If he could make a meaningful difference in internal audit, 30-year-old **JAD ANTANIOS** would enhance internal audit knowledge sharing worldwide to "make information available to those who want to invest in themselves" and help further the practice of internal audit in developing countries. Indeed, the Damascus University graduate, who is now in charge of internal audit operations at a financial institution in the Middle East, established the internal audit department at an insurance company before moving to his current position. One of his colleagues says of Antanios, who's currently pursuing the Certified Financial Services Auditor designation and the Certification in Risk Management Assurance, "He's one of the best leaders I've ever worked with. He understands the strengths and weaknesses of his subordinates, and he knows how to delegate tasks to them accordingly." Co-workers also credit him for creating loyalty and strength within his audit group, and for having a sense of humor that helps maintain group morale. He plans to keep putting those attributes to good use: "In the next decade I see myself leading and promoting the internal audit profession through an IIA chapter my colleagues and I are seeking to establish here, or by heading an internal audit function in a way that we become a practice benchmark in the market." He hopes to accomplish that and keep a smile on his face at the same time. "I always try to be that friendly, approachable person who gets the job done smoothly while maintaining a sense of humor," he says.

"I always try to be that friendly, approachable person who gets the job done smoothly while maintaining a sense of humor."

MORE To read about the Emerging Leaders honorable mentions, VISIT www.InternalAuditor.org

Choosing the Leaders

The Emerging Leaders were selected by a panel of judges comprising some of the most distinguished audit professionals in the industry. Panelists volunteered their time to review the many nominations *Internal Auditor* received and chose the practitioners they felt best represent the profession's bright future. Nominees were judged in six broad areas: professionalism, leadership, certifications, advocacy, community service, and innovative thinking.

Michael Cowell, CIA, is senior managing director and chief auditor at TIAA-CREF Financial Services and vice chair, finance, of The IIA's North American Board of Directors.

Nancy Haig, CIA, CFSA, CCSA, CRMA, is director, Internal Audit & Compliance, at Global Consulting and a member of The IIA's Publications Advisory Committee.

Katie Houston, CIA, is assistant city auditor at the Austin City Office of the City Auditor, an IIA Emerging Leaders Task Force member, and a 2013 Emerging Leaders honoree.

Princy Jain, CIA, CCSA, CRMA, is a partner at PricewaterhouseCoopers and senior vice chair of The IIA's North American Board of Directors.

Seth Peterson, CIA, CRMA, QIAL, is internal audit manager at The First National Bank in Sioux Falls, an IIA Emerging Leaders Task Force member, and a 2013 Emerging Leaders honoree.

Harold Silverman, CIA, CRMA, QIAL, is vice president, Internal Audit, at The Wendy's Co. and vice chair, professional certifications, of The IIA's Global Board of Directors.

Renato Trisciuzzi, CIA, CCSA, CRMA, QIAL, is corporate audit director at Walmart and secretary of The IIA's Global Board of Directors.

Angela Witzany, CIA, CRMA, QIAL, is head of Internal Audit at Sparkassen Versicherung and senior vice chair of The IIA's Global Board of Directors.

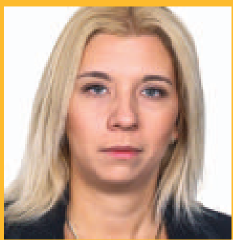
JAMIE WILSON is something of an expert on the U.S. Sarbanes-Oxley Act of 2002. The 30-year-old Texas A&M University graduate has led her Sarbanes-Oxley team through a period of great change, colleagues report, as GM Financial began to align its Sarbanes-Oxley program with that of the parent company when it was acquired as a subsidiary in 2010. She managed the change effort while keeping team morale high through transparent communication and ensuring the team had the resources needed to overcome the challenges it faced. Not only did the Ft. Worth, Texas-based Wilson and her team get the job done, they produced a work product that achieved maximum reliance from external auditors—and excellent outcomes for management. In fact, she says her favorite aspect of the job is the sense of accomplishment she experiences from helping her team reach its deadlines. "I am proud that my team's work provides comfort to our executives about the functioning of our internal controls," she says. Wilson actually interned with GM Financial—formerly AmeriCredit—in internal audit as a junior in college. "I really enjoyed the internal audit team and the nature of the work," she says, "so I was thrilled to be offered a full-time position when my internship ended." She's been in internal audit full time since January 2007, working in operations audit until 2012, followed by a brief stint in continuous audit until transitioning to her current role on the compliance audit team in early 2013. She adds that her current boss, Vice President–Compliance Audit, Internal Audit, Laura Eakin, is her mentor: "She is great at knowing what to say and how to say it—especially in challenging situations."

ASSISTANT VICE PRESIDENT–COMPLIANCE AUDIT, INTERNAL AUDIT
GM FINANCIAL

Jamie Wilson
CIA, CPA, CFE

"I am proud that my team's work provides comfort to our executives about the functioning of our internal controls."

ON THE **RISE**



Maja Milosavljevic

CIA

“The combination of traditional knowledge and ... technology is best for modern practice.”

SENIOR INTERNAL AUDITOR
ERSTE BANK A.D.

The aspect of internal audit that many practitioners dread is actually **MAJA MILOSAVLJEVIC’S** favorite: presenting results to clients. “The results often contain findings and recommendations for improvement of business processes that the clients have not been aware of,” the 29-year-old Belgrade, Serbia-based practitioner explains. “Clients and management can directly see the significance of internal audit work and acknowledge how internal audit helps and improves the whole organization.” Where that’s not the case, she’d like to make it so. She says most people are still not fully aware of internal audit’s potential and its role as a trusted adviser. “Finding and using various new ways of presentation, quantification, and description of results achieved would be very helpful.” Milosavljevic has been involved in audit since college. After graduating from the University of Belgrade Faculty of Economics in 2009, she started her career at Deloitte Serbia performing mainly external audit work. She transitioned to the National Bank of Serbia’s Internal Audit Department, then back to Deloitte for a spell in internal audit, and then to her current position. As well, she’s pursuing a PhD in economics and a Chartered Financial Analyst designation. Milosavljevic likes to pass her expertise on to colleagues both less and more experienced than she. “I have had experience with reverse mentoring, and I find it very good for everyday work,” she says. “The combination of traditional knowledge and experience with knowledge about the modern world of social media and other forms of forward-thinking technology is best for the modern practice of internal auditing.” Ultimately, she’d like to keep exchanging knowledge by starting her own internal audit consulting company one day.

When **ANDREW LOYACK** sets his mind to something, there’s a pretty good chance it’s going to happen. At home, the 29-year-old confessed foodie and his wife set out to improve their health last year, and together they’ve lost 125 pounds. At work, he wants internal audit to “take full advantage of computerized data collection and analysis techniques to help identify control weaknesses.” The technology, he says, can help auditors explain issues more clearly to clients and provide meaningful suggestions to change the audience’s perception of internal audit’s value. He accomplishes this as an outsourced internal auditor helping several community banks. “My favorite aspect of this job is helping clients of various sizes and complexities find efficiencies and stronger controls to better their internal control structure,” the Camp Hill, Pa.-based Shippensburg University graduate says. He also points out that his co-workers are his role models and mentors. “Each day I learn something new from my co-workers: tried-and-true lessons from seasoned teammates and new technical skills and different points of view from less-tenured staff.” He adds that, despite regulatory changes shaking up the industry and changes in the way consumers bank, his ambitions will likely stay the same—no matter how much his environment changes. “Regardless of where I end up, I hope I am able to continue to use my internal audit and IT auditing skills to identify efficiencies, fraud, and control breakdowns so that the internal control structure can remain strong.”

“My favorite aspect of this job is helping clients ... find efficiencies and stronger controls.”

MANAGER
FINANCIAL OUTSOURCING SOLUTIONS

Andrew Loyack

CFSA, CISA

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

"Being a ref helped me develop soft skills… not to mention a pretty thick skin."

Matt Beachnau
CISA, CTGA

MANAGER
PROTIVITI

You can learn a lot from student athletes. During his years at Indiana University Bloomington, **MATT BEACHNAU** put himself through school in part by working as an intramural sports referee for basketball, volleyball, and softball. "Besides encouraging my love for sports," he says, "being a ref helped me develop soft skills for conflict resolution—not to mention a pretty thick skin." Off the court, the 29-year-old says his favorite aspect of internal audit is that each day "brings something new." Beachnau points to the opportunity many audit practitioners have to work with people from all different backgrounds, industries, and parts of the world. "That helps keep each project engaging and fulfilling, because each one presents its own unique set of challenges and experiences," he says. One experience the Indianapolis-based Beachnau enjoys is educating. "For the past three years, I have been involved in developing and presenting an internal audit two-day training curriculum for a financial services client," he says. Attendees include internal audit staff plus senior management in audit and compliance; the mini-course includes presentations on IT audit techniques, social media, and audit soft skills. And he participates in Protiviti's internship program, helping incoming interns manage their schedules, advocating for them, and working with clients to ensure that interns can participate in real-time projects. As well, he's pursuing The IIA's Certified Financial Services Auditor qualification. His aim? To change the view of an internal auditor as someone who simply follows a work program, exposes issues, and "causes further headaches." To do so, he endeavors to develop and nurture relationships with the management representatives involved in each audit so that practitioners are seen as advisers, not adversaries.

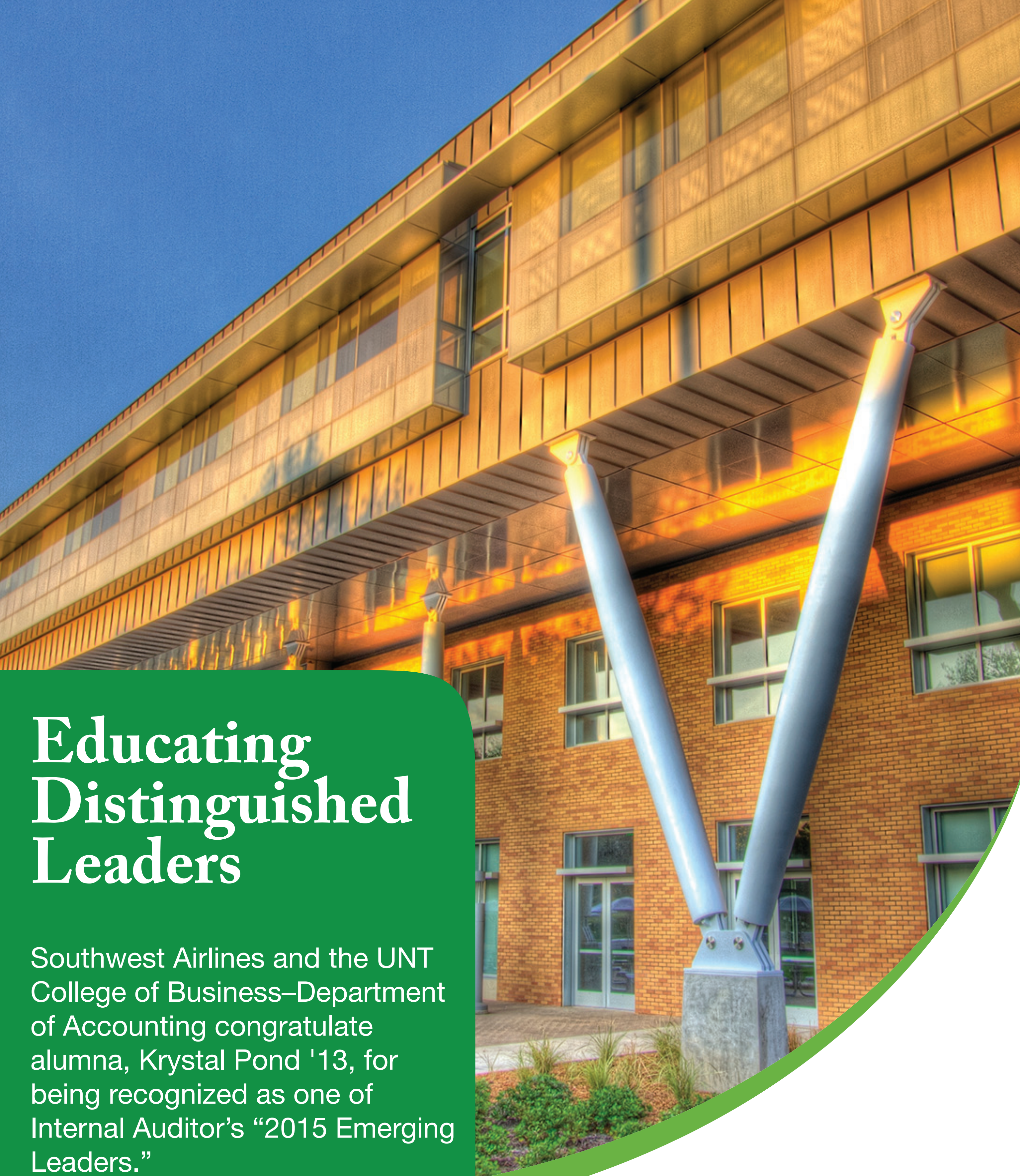
MORGAN ABSHIRE has learned that a college course may not best represent professional reality. She started in accounting directly out of high school and, before joining the internal audit staff at the casino she works for now, she applied for a staff accountant position. "When I interviewed, they brought to my attention the internal audit position, but I wasn't sure of the area and, to be honest, it wasn't exactly the most interesting subject in college," the McNeese State University graduate says now. But when she was interviewed by the internal audit manager, the Lake Charles, La.-based 29-year-old, who's pursuing Certified Internal Auditor certification, says she left the office knowing that internal audit was where she wanted to start her career. "Here I am six years later," she adds, "same department and same company." Moving forward, Abshire hopes to be an internal audit manager or director—or something more specialized, such as a data analytics senior auditor for the entire company. "I absolutely love performing data analytics, which is my favorite thing about internal audit," she says. Indeed, she's said to have become "obsessed with developing an audit script that would help her organization automate its compliance requirements for the U.S. Bank Secrecy Act and Title 31." She worked for countless hours troubleshooting scripts until she developed one that detects specific suspicious activities. Now she's developing individual scripts for 14 other properties. More broadly, she loves the fact that her work is constantly changing—even in an industry that is highly regulated. "The casino industry is continuously evolving," she says, "which provides new opportunities and challenges, including new risks. I get to learn new things with every audit I perform." ia

SENIOR INTERNAL AUDITOR
PINNACLE ENTERTAINMENT

Morgan Abshire

"I absolutely love performing data analytics, which is my favorite thing about internal audit."

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



The Versatile Auditor

Diverse backgrounds can provide different perspectives, help bridge the skills gap, and strengthen the audit team.

Thomas C. Sanglier II

Now is a great time to be an internal auditor. Stakeholders recognize the value internal auditors bring, audit projects are more challenging, and there is increasing demand for internal audit's work. In fact, the number of job openings for internal auditors posted on The IIA's Audit Career Center has more than doubled from a year ago, while the number of résumés posted by job seekers is down 42 percent. Richard Chambers, president and CEO of The Institute, says that companies are facing the most severe internal auditor shortage in more than a decade, calling it "a classic supply-and-demand dilemma."

The IIA's 2015 Pulse of Internal Audit survey, along with perspectives from CAE interviews, note that one reason for the growing talent shortage in the profession is that internal audit functions continue to seek talent with skills and competencies in the traditional areas of accounting and finance, despite shifting expectations from audit committees to address critical risks outside of these areas.

How can the internal audit profession and, specifically, department leaders meet the growing demand for internal auditors cost effectively while maintaining or even increasing quality? One answer is to broaden talent pool strategies to include nontraditional internal auditors; specifically, those with training and experience in other disciplines such as engineering, human resources (HR), legal, and supply chain.

Raytheon Internal Audit is proud to have an Emerging Leader recognized by *Internal Auditor* magazine each of the past three years. One of this year's honorees, Marbelio Villatoro, an integrated project manager, is one of many Raytheon nontraditional internal audit team members. In other words, he did not study for, or begin, his successful career as either an external or internal auditor. Neither did three Emerging Leader honorable mentions — Lara Olisky, Maureen O'Connor, and Meghan Kennedy — one of whom was an engineer by training and work experience before joining the internal audit department.

> **Nontraditional auditors can improve a project team's risk assessments, data gathering, and interpretation of results.**

DIVERSE AUDIT TEAM BENEFITS

In addition to increasing the number of potential candidates, seeking out nontraditional internal auditors can bring significant benefits to any department. Organizations with more diverse workforces perform better financially, according to a 2015 research study by McKinsey and Co. Researchers stated that "[m]ore diverse companies … are better able to win top talent and improve their customer orientation, employee satisfaction, and decision-making, and all that leads to a virtuous cycle of increasing returns." Typically, diversity is thought to mean different genders, race, or age. However, diversity also applies to different experiences, education, and training.

Consider the differences between a classically trained and a nontraditional auditor. A classically trained internal auditor often has the desired audit skills critical to delivering projects that meet professional standards. Often, classically trained auditors have taken college-level classes in internal auditing or spent time with a professional audit firm, which can provide valuable perspective on other audit functions or industries. A nontraditional auditor often comes from another department within the organization, with knowledge of organizational and industry risks, key processes, and useful networks. Based on their knowledge and experience, nontraditional auditors can improve a project team's risk assessments, data gathering, and interpretation of results.

Just as an engineer can give a different perspective on a problem or subject, a balance of classically trained and nontraditional auditors can increase the diversity of thought on almost any topic. As these nontraditional auditors learn about audit methodology, the classically trained auditors will similarly enhance their knowledge of organizational functions and processes. At Raytheon Internal Audit, the audit team has included team members with backgrounds in engineering, supply chain, HR, legal, finance, and IT. All have been valued members of the team, contributing to outstanding audits

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

as well as improvements in internal audit processes.

A well-balanced team also can positively impact the internal audit brand. At Raytheon, the backgrounds of the audit team are shared with audit clients at the start of each engagement. A diversified team that includes auditors who come from different areas of the organization generally results in a higher level of customer respect for the audit team.

RECRUITING AND RETAINING

Many nonauditors do not understand what internal audit is or does. So, successful recruiting starts with quality marketing. Regardless of the chosen career path of the audit team, today's internal audit function has to be about building business leaders, not auditors. This message has to be a constant and consistent part of a marketing strategy. Marketing strategies can include:

- Working with HR and communications to create or refresh existing departmental materials. At Raytheon, internal audit created a four-minute video describing the department and the internal audit experience, which included testimonials from customers and alumni.
- Participating in, and leading, non-audit-related organizational initiatives. For example, involvement by team members in company diversity efforts and employee resource groups provides nonauditors a different, positive interaction with the internal audit team.
- Finding every opportunity to present within the organization at events such as new-hire training, leadership training, and nonaudit departmental meetings.
- Blogging or contributing material to the organization's website, intranet, newsletter, or other communication vehicles.
- Talking to senior leaders about internal audit opportunities for their high-potential employees, and the benefits they will gain after a short rotation in internal audit. Create a formal or informal rotation program or guest auditor program.
- Loaning top internal auditors to senior leaders for help on short-term assignments.
- Creating and distributing a newsletter to share with the audit team as well as internal audit alumni, and ask that they share with others outside of the department.
- Being available for career conversations and mentoring with anyone inside the organization.
- Inviting employees outside of the internal audit function to participate in audit projects (with their supervisor's permission), whether as auditors or as observers and advisers. This can help expose

RECRUITING CHALLENGES

Forty percent of respondents in the The IIA's March 2015 Pulse of Internal Audit survey, Navigating an Increasingly Volatile Risk Environment, indicate that attracting and retaining talent is a high or critical priority for their audit plan. Furthermore, 54 percent of survey participants cite competition for a limited pool of skilled auditors as the reason for skill gaps on their teams.

Fifty-six percent of respondents say they are recruiting talent from outside internal audit to address the skills gap. Though this means a wider talent pool to choose from, it also means more competition. To appeal more to potential talent, 39 percent of participants are offering on-site training, 23 percent are offering a more attractive salary, and 19 percent offer internal employee rotational programs.

While organizations are looking for more internal auditors, stakeholders are looking for more value from them. Consider the changing required competencies needed to be an effective internal auditor. Analytical and critical thinking and communication skills are the top two skill categories, with 96 percent of Pulse survey respondents considering them to be either very or extremely essential; business acumen skills and industry-specific knowledge also were rated highly. Technical audit skills were not at the top of the list.

SEE "On the Rise" on page 30 to read about the 2015 Emerging Leaders.

Talent is cited as a top barrier by **65%** of stakeholders who do not find value in their internal audit department, according to PricewaterhouseCoopers' 2015 State of the Internal Audit Profession report.

them to what internal audit does and stretch or develop their skills. For formal recruiting, do standard job requisitions require specific internal audit or finance experience, certifications, or education? Consider deleting these requirements to avoid discouraging highly talented candidates from applying. Adjust requisitions and job postings so they focus on competencies rather than experience and training. Ensure that internal audit leaders and the recruiting team understand the focus on competencies.

Another challenge in recruiting a nontraditional auditor is finding someone willing to sacrifice months or years away from their chosen field of interest. Fortunately, many high-potential employees are looking for opportunities to broaden their skills and learn more about the organization. Some are looking to change careers entirely. Retaining these employees becomes easier when time and resources are invested in helping them develop their professional skills.

If the department's mission is to truly develop business skills and leaders, then a rotation in internal audit should be viewed as a career benefit or an opportunity to redirect. The existing internal audit team, as well as recruiters, should be able to articulate with conviction how experience in internal audit will benefit the candidate, regardless of his or her ultimate career path.

Internal audit leaders should actively share this message with senior management to ensure their support of any candidate who applies. Giving up top talent is hard for any leader, so focus on leaders who put their team members' careers first. Obtain a commitment from those leaders that they will stay engaged in the development of the team member during his or her internal audit rotation, and will bring the employee back to his or her team at the end of the rotation (or sooner if circumstances warrant). Honest, transparent communications and agreements with both the recruit and his or her leader will greatly ease potential concerns for all parties.

Quality onboarding and training of any new employee is critical for his or her long-term success. A nontraditional hire will require additional training, specifically in the areas of internal audit methodology and professional standards. This can be accomplished through formal introductory audit training.

Formal training should be supplemented with focused on-the-job training and timely feedback. Assigning a specific, skilled mentor to help the new hire can be beneficial. This is also an opportunity for existing team members to develop their mentoring skills. However, equally important is the opportunity for internal audit leaders to receive reverse mentoring. Assuming curiosity, continuous learning, and courage are on the department's list of desired competencies, it should not be surprising that nontraditional auditors will challenge thinking and established processes. This reverse mentoring should be encouraged, even if the initial ideas are of questionable value.

Raytheon Internal Audit requires every new hire, regardless of his or her background, to obtain the Certified Internal Auditor certification within two years of hire. In addition to demonstrating competence, preparing for the examination helps expedite a new hire's knowledge of professional standards and audit techniques.

When staffing nontraditional auditors on engagements, consider their project preferences to help demonstrate the department's commitment to their growth as a future business leader consistent with the marketing and recruiting messages. Careful selection of the first and second assigned projects, and their immediate project supervisor, will also speed development of internal audit skills. However, schedulers also must carefully consider restrictions to prevent impairment of objectivity, both in appearance and in fact.

Internal audit functions with diversified skills are adding more significant value than those lacking such diversity.

IT WON'T BE EASY

There is a need for internal audit to expand its skills. In PricewaterhouseCoopers' 2015 State of the Internal Audit Profession report, researchers found that "nontraditional skills are helping the most-valued internal audit functions make the journey successfully." Internal audit functions with diversified skills are adding more significant value than those lacking such diversity. If carefully hired, trained, and supported, nontraditional auditors can cost effectively increase the value internal audit delivers to its customers. However, building a robust pipeline of eager, nontraditional auditors takes time and effort. But the benefits are well worth it. Ia

THOMAS C. SANGLIER II, CIA, CPA, CRMA, *is director of internal audit at Raytheon Co. in Waltham, Mass.*

Public sector agencies are trying to gain their balance as they navigate the obstacles to implementing enterprise risk management.

Governing Government

Risk

Jane Seago

Illustrations by Gary Hovland

The Association for Federal Enterprise Risk Management (AFERM) and PricewaterhouseCoopers recently queried U.S. federal risk management practitioners about the state of enterprise risk management (ERM) in the government. Through surveys and interviews, these professionals provided a broad-ranging discussion of the challenges involved in leveraging the effectiveness of their ERM program, the litany of risks they face, and the practices they have found effective and ineffective.

In fact, their comments mirrored exactly the types of concerns and opportunities regularly surfaced by corporate ERM practitioners—until one looks closer at the statistics surrounding the pervasiveness of the ERM function. Whereas risk management programs are a common feature on the corporate landscape, 44 percent of the government participants report that their agencies still do not have a formal ERM program. Those that do have a program indicate that it is relatively new: five years old at the most. Taken together, those two data points raise the question of why ERM isn't as well entrenched in government entities as it is in the private sector.

Goli Trump, auditor general for the Fairfax County Public Schools School Board in Fairfax, Va., cites a difference in the speed with which government entities in the U.S. adapt to change. "ERM is a discipline," she explains. "But it is most successful when it entails a cultural change, and cultural changes tend to take hold faster in private organizations because they thrive on change. Change takes longer in the public sector."

Regardless of its pace, change invariably involves a life cycle, and government internal auditors are involved at each phase of that process for ERM. At the inception, someone in an agency—perhaps department management, sometimes the

KAREN BOLT/FAIRFAX COUNTY PUBLIC SCHOOLS

"Large government settings are inherently segregated when it comes to policy implementation and execution at the operating level."

Goli Trump

"In state government responsibility [for risk management] is shared across functions, reporting channels, and traditional lines of authority."

Melinda Miguel

internal auditor—suggests that the agency needs a more formal way to think about and manage risk. In many government entities, the internal auditors are the risk experts, so they are consulted to help define the approach.

As the life cycle progresses, internal auditors engage in defining the program's goals, educating the agency's staff about risk, or suggesting a framework to use, while avoiding making management decisions that might affect their objectivity later. Then, as the program matures, they transition to the more traditional activities of assessing risks and the risk management program itself.

APPLES AND ORANGES

Although both businesses and government entities manage risk in their daily operations, there are differences that make implementing ERM more complex for governments, says Karen Hardy, an author and expert on federal government risk management in Washington, D.C. "In private industry, you can implement ERM programs just within your specific company, so in that sense it moves forward faster," Hardy notes. She compares the private sector's more contained approach to the government's tendency to move in clusters, adding, "There are many regulations and government agencies to consider. An across-the-board policy could impact the whole, and even just a portion of, federal government agencies."

Although Joseph Picolla, director of management advisory services with the U.S. House of Representatives Office of Inspector General in Washington, D.C., points out that broad statements do not always apply—for example, certain areas of the government think about risk all the time—he agrees that challenges to ERM in government agencies exist. "The government is structured so differently from the private sector," he explains. "Given the diversity of missions, purposes, and priorities represented by different government agencies and departments, it is not always possible to make direct, apples-to-apples comparisons to companies."

The AFERM survey respondents report a laundry list of challenges they face in instituting ERM functions and risk practices in their own agencies. They cite the difficulty of building business cases to justify the funding needed to implement an effective program, and they bemoan the lack of executive buy-in required to achieve the expected benefits and prove an ample return on the investment. But, without question, the largest hindrance to implementing an ERM program identified by the AFERM survey respondents is silos: in data, decision-making, and existing risk management approaches. Trump concurs. "Large government settings are inherently segregated when it comes to policy implementation and execution at the operating level," she says.

The largest hindrance to implementing an ERM program is silos.

CHALLENGES OF MULTIPLICITY

The issue of multiplicity—in virtually every aspect of government—is a recurring theme, as efforts to implement ERM wrestle with the need to juggle a broad range of not-always-compatible priorities. "Managing risk in the private sector and in the public sector is a shared responsibility in and throughout an enterprise," says

58% of respondents say their department has integrated ERM into strategic planning, and 82% say ERM can help them achieve their goals, reports PwC's Enterprise Risk Management in the Public Sector survey.

Melinda Miguel, chief inspector general with the Florida Executive Office of the Governor in Tallahassee. "However, enterprise lines in the private sector are more clearly delineated. In state government, responsibility is shared across functions, reporting channels, and traditional lines of authority."

Even something as fundamental as mission provides an area where multiplicity raises challenges relative to an effective ERM program. Private-sector companies generally exist for one primary purpose—generating revenue. But governments exist for a variety of nonrevenue-focused reasons. They promote welfare, protect people, and address a social good or need. Each of these purposes must be reflected in the ERM program. "Governments' multiple purposes can be accomplished in many different ways, involving different risks and goals," Picolla explains. "One part of the government is trying to cure illness; another part is fighting terrorism. Each agency's ERM program has to take this diversity into account."

Miguel agrees. "Not all government operations and programs can be managed by profits or return on investment or by using a traditional economic and efficient focus on operations," she says. "A sound ERM approach must consider all areas of focus, competing priorities, and differing social or moral benefits vs. the traditional focus on the bottom line."

Sometimes there is not even one simple, straightforward purpose within a single agency. That's the case for the Virginia Department of Alcoholic Beverage Control. "My agency is in the initial stages of implementing ERM, so we are in a transition state, compounded by our unique double mission," John Wszelaki, director of internal audit for the Richmond-based department, explains. "We are in the retail business of selling alcohol, yet we are also responsible for the enforcement of all laws in the Commonwealth related to alcohol. We exist in a delicate balancing act: sales vs. responsible consumption." The agency is addressing the situation by using education to teach employees what ERM encompasses, how the various departments should view risk in light of the double mission, and how every component of the operation has a role in risk mitigation.

Not even basic definitions come easily in a government setting. Picolla notes, "The E in ERM stands for enterprise. In the government, what does that mean? Is it the department? The agency? The entire government?"

PEOPLE AND POLITICS

As with many programs, one critical success factor is managing the people involved. Sometimes this entails first getting a handle on who those people are and how many there might be.

Thomas O'Connor, a consultant from Alexandria, Va., and a retired auditor with the Government Accountability Office, the U.S. Agency for International Development, and the Peace Corps, points out the greater range of stakeholders government risk managers must address. "The citizens are increasingly empowered, through public access to reports and sources, and open meetings and hearings, to become an active part of the process," he says. "And don't forget the media. It tends to focus heavily on every governmental flaw it can find, and too often does not put issues into perspective." Ultimately, O'Connor says the potential impact of the risks involved and the engagement of a large and diverse body of citizens served by the government combine to create "a degree of magnitude vastly different from that faced by most companies."

It is impossible to talk about government risk without mentioning politics. People in elected and appointed positions inherently carry portfolios of differing priorities. "Coming to consensus involves a legislative process. It isn't easy or quick, and it requires a lot of compromise," Picolla says. "Ultimately

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

"Government programs have a much greater number and variety of objectives than the private sector."

Thomas O'Connor

"Internal audit should participate in influencing how risk is approached as well as evaluating how well risk is mitigated throughout the organization."

John Wszelaki

the question is: Where do we apply resources first?"

INTERNAL AUDIT IN GOVERNMENT ERM

In an environment riddled with reporting and compliance laws, multiple priorities and goals, high degrees of risk, layers of governing bodies, and a large and involved stakeholder base, internal audit clearly has a significant role to play. In addition to the traditional activities of evaluating risk management processes, giving assurance on risks and related processes, and evaluating risk reporting, internal audit can champion the ERM program, coach staff on risk, promote a shared understanding of the importance of risk management and controls, and assist management in determining optimal ways to mitigate particular risks.

But these activities aren't exactly the same as those performed in the private sector, according to Picolla. "In the federal government, there are no entities called 'internal audit,'" he says. "They are called inspectors general, but their function is largely the same. They do performance audits and assurance audits, as done in companies, and some provide advisory services. But one difference is that some inspectors general, especially in the executive branch of the government, also perform investigations, which can lead to criminal charges." Safeguards are in place to preserve segregation of duties and protect against conflicts of interest, he points out.

As in private companies, the size, complexity, and needs of the government organization and the maturity level of the ERM program dictate internal audit's involvement. Wszelaki's department is an example of a mature program at the state level. He describes internal audit's role in his agency as "leading the discussions with the executive management team on many things related to ERM." That involves conversations ranging from the basics to high-level strategy: what ERM is, the role everyone plays in risk evaluation and mitigation, the value of everyone's input, the effort to reach agreement on interrelated risk and identify who has ownership of the mitigation strategy, and the acknowledgment that risk is a component of all strategic decisions the agency makes.

Government executives and internal audit have a common goal, the organization's success, Hardy notes. "You need a balance of both to ensure that the organization isn't overlooking any blind spots, both in what has already occurred and in what can happen as you move forward," she says. "The internal audit and management communities, working together, balance that out."

In any environment, the balancing act performed by internal audit is hardly a minimal-effort activity. However, O'Connor says internal audit in a government setting is subject to an even greater workload. "Government programs, and the agencies and departments that operate the programs, have a much greater number and variety of objectives than the private sector," he observes. "This is reflected in performance reporting. The private sector has a shorter and more defined list of performance metrics, such as market share or profit margin, whereas many government agencies and departments use and report on hundreds of measures arising from the number and diversity of program activities."

Trump says she thinks of ERM and internal audit on a continuum at a very high level. "I like to ensure that my agency has applied all the phases of risk analysis before it considers auditing the performance of any risk mitigation activity, vis-a-vis internal controls," she explains. "My experience is that auditors welcome effective risk analysis done by the audited entity."

Visit our **MOBILE APP** + **InternalAuditor.org** to watch a video synopsis of public-sector findings from The IIA's 2015 CBOK research.

FRAMEWORKS AND GUIDANCE

Government internal auditors have a variety of guidance documents available to help steer their department's ERM programs. Among those frequently used are:

- **OMB Circular A-123 – Management's Responsibility for Internal Control** (updated in 2015, to become effective in fiscal year 2016). The U.S. Office of Management and Budget (OMB) guidance encourages agencies to incorporate risk management into their operations, beginning with an assessment of risk appetite and tolerance in support of mission achievement. It further requires agencies to look for opportunities to do things differently – perhaps even to take new risks to maximize benefits – as opposed to focusing solely on stopping negative outcomes.
- **The Committee of Sponsoring Organizations of the Treadway Commission (COSO) *Enterprise Risk Management-Integrated Framework*** (2004, update underway). The COSO ERM framework is used by agencies to enhance their ability to manage uncertainty, determine an appropriate level of risk to accept, and improve understanding of opportunities to provide stakeholder value. It includes tools to help management report risk information and review and assess the application of ERM.
- **ISO 31000: 2009 – Risk Management – Principles and Guidelines** (2009). The International Organization for Standardization (ISO) guidance's principles, framework, and process for managing risk can help agencies achieve their objectives, improve their identification of opportunities and threats, and allocate and use resources for risk treatment. It also provides guidance for internal and external audit programs.
- **Government Accountability Office (GAO) – Risk Management Framework** (2005). The GAO framework provides a full cycle of related activities, covering strategic planning through implementation and monitoring. It can be used to inform agency officials and decision-makers of the basic components of a risk management system, or it can be used as a stand-alone guide. It is designed to be flexible, so the approach may be applied at various organizational levels, from a department of a multi-agency organization to a specific project or program.

Miguel sees internal auditors as change agents who can identify and advise management of emerging risks such as information security, cyber preparedness, and fraud. Moreover, they can facilitate cross-agency approaches to mitigate risk, develop key partnerships to address overarching risk issues, and break down barriers to communication about risk. "Internal auditors hold a position of influence because of to whom we report, our reports, and the function that we have to question operations," she emphasizes. In her view, internal auditors can add value to the ERM program by providing both assurance and consulting services relative to risk, always in keeping with the *International Standards for the Professional Practice of Internal Auditing* dealing with objectivity. "If we don't challenge ourselves to continually improve our services, we will become irrelevant or even obsolete," she asserts.

Wszelaki also sees the potential for an expanded role for internal audit in ERM. "Internal audit should participate in influencing how risk is approached as well as evaluating how well risk is mitigated throughout the organization."

THE VIEW AHEAD

Despite the general consensus that the private sector is leading the way in ERM, there is equal agreement that government entities are picking up the pace. According to O'Connor, "The federal government — through its central management agencies such as the Office of Management and Budget — has signaled that ERM is on its way. I know from my contacts with federal employees that several federal agencies' ERM policies are already emerging, and they are beginning to assign real resources to ERM."

Trump agrees, but recognizes the challenges in a government setting. "Managing high risks while at the same time driving strategy and performance may be less clear than in the private sector," she admits. "Still, it's doable."

In today's threat-laden environment, there is likely little choice in the matter. Operating without an ERM program is a risky business in itself, and cannot be mitigated by writing a few policies and practices that then gather dust on a shelf. In a connected world, if one entity is at risk, all are at risk. "Everyone, whether in the private sector or public sector, has a role in identifying, detecting, mitigating, managing, and communicating risks, regardless of the degree of the ERM program's sophistication," Miguel avows. "We are all in this together."

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

STAKEHOLDER RELATIONSHIPS

The Trusted Adviser

Internal audit can change stakeholders' perceptions by being more reliable and credible, and strengthening relationships.

David Linnard
Mike Kinney

David Smart, the audit committee chairman at MEK Corp., called a meeting with the company's CAE, Michael Smith. "Michael, please highlight for me internal audit's accomplishments during the year," Smart requested. "And describe how you and your team have reached out to gain the respect of executive and line management. Do your team members understand the corporate strategy, the way the company is governed, and the most significant risks the company faces? Does your audit plan align with this understanding? Do you believe our executive leadership understands how internal audit can add value?"

Smith's blank stare suggested he was not prepared to answer these questions. The following month, Smith learned that MEK would be outsourcing its internal audit function. Internal audit had been caught up in measuring its performance based on the standard metrics such as the number of audits completed, the number of findings, and basic compliance activities. The audit committee's position was that this basic type of audit work did not address the company's compliance, operational, and strategic risks, and could be outsourced cost-effectively. It didn't perceive that internal audit was engaged with the business in a way that would merit its inclusion in management meetings and strategy discussions.

In this fictional scenario, Smith could have seen a different outcome if his internal audit function was considered a trusted adviser by all of its stakeholders. Many internal audit departments aspire to be trusted advisers and encapsulate similar aspirational language into the department's vision and mission statements or audit charter, but fail to achieve or sustain that status.

David Maister, Charles Green, and Robert Galford introduced the concept in their 2000 book, *The Trusted Advisor*, to enhance client relationships. The fundamental principles of the Trust Equation they developed can be applied to improving internal audit's understanding of its relationship with its stakeholders and potentially enhance the audit function's performance. But this requires thinking about internal audit in a different way.

SHAPING THE PERCEPTION OF INTERNAL AUDIT

The ease or difficulty of the trusted adviser journey is influenced by an important determinant that is outside of internal audit's control—how the department fits within the organization's governance structure. Does internal audit truly operate as the third line of defense in the organization's response to risk? From where does internal audit receive the broad delegation of authority that defines its role and accountabilities—to whom does it report? Is it the audit committee, the CEO, the chief financial officer (CFO), the chief operating officer—or is it some combination of reporting lines that compromise both independence and the wider understanding of its role?

The current recommendations for internal audit to report administratively to the CEO or CFO and functionally to the audit committee establish the ideal environment for the audit function to achieve trusted adviser status. Internal audit needs to establish such trust to ensure that the first and second lines of defense understand and support its independent, third-line role.

On the journey to becoming a trusted adviser, the internal audit department must create a brand identity that all stakeholders, including the audit team members, buy into and understand. This may require discussions to expand the remit of the function, which may need to come from the top down. But before embarking on such a journey, a level of self-awareness and honesty about the current state of the function is required. The Trust Equation can facilitate this self-realization.

THE TRUST EQUATION

The Trust Equation has four components that define the level of trustworthiness of an individual or entity (see formula on this page). Focusing on each component in the context of what internal audit does can identify strengths and weaknesses that define the level of trust that stakeholders have in internal audit.

$$\text{TRUSTWORTHINESS} = \frac{\text{Credibility} + \text{Reliability} + \text{Relationship Strength}}{\text{Self-interest}}$$

Credibility is established in the realm of words. Are the audit department and individual auditors considered believable and trustworthy? Internal audit might expect to hear comments such as, "I can trust what this auditor says about …"

Reliability is established in the realm of actions. Do the audit department and its

TO COMMENT on this article, EMAIL the authors at david.linnard@theiia.org

staff present themselves as dependable, honest, and consistent? Internal audit might expect to hear comments such as, "I can trust this auditor to do …"

Relationship strength is established in the realm of emotions. Is the internal audit department building strong relationships with the business? Internal audit might expect to hear comments such as, "I feel comfortable discussing this issue with the auditor because he or she understands my business dilemmas."

Self-interest is established when the department's or individual internal auditor's actions and behaviors are self-promoting, rather than in the best interest of stakeholders and the organization as a whole. If internal audit's stakeholders sense a high level of self-interest, it will quickly undermine its trustworthiness. When self-interest is low, internal audit might expect to hear comments such as, "I can trust that this auditor cares about how well my control environment is operating and that the outcome of audit work aligns with, and supports, the success of my business."

By looking at the Trust Equation through the lens of behaviors associated with internal auditors, it is easy to see how these behaviors can support or detract from becoming a trusted adviser.

CREDIBILITY

Being credible is not simply about having the right technical expertise, which can easily be measured by certificates and diplomas, but it also relates to experience and personal attributes such as presence or gravitas. Outstanding technical competence is necessary but not sufficient.

Credibility results from being recognized by stakeholders as reasonable, understanding, and committed to beneficial outcomes for the organization. The audit organization must be staffed with the right balance of individuals who have experience working in the business and understand its objectives and the dynamics that come with reaching them, and those with a strong audit pedigree.

Credibility increases when a CAE has built strong relationships with senior executives and communicates powerfully about internal audit's role within the organization's governance framework (third line of defense). Auditors need to be able to communicate this purpose, as well. The audit department should not second-guess the decisions line management makes that affect business outcomes. Instead, it should see its primary role as ensuring that business is performed within the boundaries of the risk appetite set by the board and CEO. To do this, internal audit must use its understanding of the organization's enterprise risk management model to shape the audit plan and be responsive to new risks as they emerge.

Internal audit should continue to bring fresh perspectives to the business and transfer leading practices across the organization. Some examples include adding an engineer who is an expert in Lean process management to the team on a rotational basis, hiring an auditor with technical experience to help optimize technology controls, and adding a human resources professional.

Once credibility is established, the internal audit department may be seen as a source of future talent for the organization. It may also become part of the career path for candidates for top executive positions.

> **Credibility is not simply about having the right technical expertise, but also relates to experience and attributes.**

RELIABILITY

Reliability requires auditors to do things in a consistent way that fosters stakeholder confidence that their findings and recommendations for improvement are fact-based. Internal audit can build its perceived reliability by consistently providing an objective perspective and focusing the audit plan on the organization's strategic, material, impactful, and emerging risks. Like the rest of the organization, the audit department must set and deliver against realistic expectations, defined by relevant metrics, and communicate these expectations to all levels of management. Additionally, auditors must be able to advise business leaders and communicate with stakeholders on a real-time basis to inform them of significant opportunities for improvement.

RELATIONSHIP STRENGTH

Some internal auditors are good at fostering relationships across the organization. Over time, these individuals can use that ability to facilitate and expedite all aspects of audit design and delivery, including conveying difficult messages in a nonthreatening way.

Auditors can improve the strength of their relationships by understanding situations and dilemmas facing stakeholders, acting like a real person—rather than someone playing a role—not sugar-coating or steering away from delivering difficult messages, and providing sound reasoning for all recommendations. Moreover, internal audit can improve relationships with the business by changing some aspects

Areas internal audit must develop to be a trusted adviser include identifying emerging risks and their business context, and maximizing technology, says EY's Governance, Risk, and Compliance 2015 survey.

of how it reports the results of its work, such as removing inflammatory terms, developing innovative solutions, clearly explaining the residual risk of each finding, and ensuring that target completion dates for management actions are reasonable, given the level of residual risk, and are agreed to quickly.

SELF-INTEREST

The denominator of the Trust Equation has only one element, self-interest. Auditors want stakeholders' perception of self-interest to be low because it is the area where trust can be most easily eroded. That is especially true when stakeholders see auditors adopting the old corporate cop mentality or acting in a way that is viewed as in the auditors' own interest or advantage. Examples include giving in to stakeholder positions simply to make audit delivery targets, showing more concern for the image of audit than the robustness of findings, and refusing to have a stake in outcomes.

Acting out of self-interest will erode stakeholder trust quickly. Trusted advisers must be seen as "servant leaders" who focus on the needs of the organization and the business units with whom they interact, acknowledge their perspectives, and provide the support they need to meet their goals.

Internal audit can achieve a desired level of low self-interest when audit staff members are more motivated by an internal drive to do the right thing than by their own personal reward or any organizational dynamic. One way internal audit can demonstrate this is by positioning the audit report as a collaborative effort to drive significant value for those who are running the business, highlighting unnecessary or unacceptable risk that the business faces. The audit report should not be merely a historical capture of what has gone wrong, which could make it difficult to reach agreement with audit clients about the findings and management's responses to them.

Moreover, internal auditors need to consider the best interests of all of their stakeholders and demonstrate that they are helping management achieve its strategies and objectives. They should work closely with the risk-focused departments in the second line of defense, while maintaining independence, to enable the organization to benefit from a truly integrated set of assurance activities.

A DIFFERENT CONVERSATION

To achieve trusted adviser status, the audit team needs to take an objective look at where they are on the continuum between corporate cop and trusted adviser. The team should then develop a road map that addresses the components of the trust equation that are required to move toward trusted adviser status.

Each step closer to trusted adviser status can enable the internal audit department to contribute more to the organization's long-term success, attract and develop top talent, and provide a more rewarding experience for those who remain in internal audit long term. That can change the conversation between the audit committee chairman and CAE to one in which internal audit is respected by the board and management, responds to emerging and strategic risks, adds value to the organization, and realizes untapped potential. Ia

Auditors want stakeholders' perception of self-interest to be low because it is where trust can be most easily eroded.

DAVID LINNARD *is principal with Assurance Advocate LLC, based in Houston.*
MIKE KINNEY, CIA, CPA, CMA, CISA, *is principal with Assurance Advocate LLC.*

Organizations should assess whether their mechanism for identifying conflicts is working as designed.

Laura Soileau
Jared Soileau

Auditing for

The alleged FIFA (governing body of soccer) bribery scandal is a recent high-profile conflict of interest scandal to be played out in the global media. Allegations of personal gain from the sale of votes to select the host countries of future World Cup events, broadcast rights, and tickets, are reminders that the risk of actual or perceived material conflicts of interest can cause significant reputational damage and can distract organizations from achieving their strategic objectives.

While the FIFA case has garnered significant attention, the media regularly reports on conflicts of interest that come to light in organizations. Conflicts of interest exist in many forms and can include transactions that directly or indirectly benefit an employee or an employee's family, relationships that may influence or appear to influence an employee in the performance of his or her job responsibilities, or an employee using his or her position within an organization for personal gain, to name a few. Given that conflicts of interest can exist in all types of industries and organizations, it is important for internal auditors to be familiar with how to audit for them.

While internal auditors need to understand the applicable standards related to avoiding conflicts of interest in their own work, it is also critical to be able to identify

Conflicts of Interest

potential conflicts of interest when conducting an engagement. In today's environment, it is important that organizations have a mechanism to identify conflicts of interest, and to periodically audit to ensure that the identification process is adequately designed and operating effectively based on the organization's specific risk factors.

BEGIN WITH A RISK ASSESSMENT

Conflict of interest audits can either be completed as a separate assessment or instituted as a standard component of various audit types, such as audits of procurement, sales, or charitable giving. Regardless of how internal auditors decide to structure the conflict of interest audit, they should begin by performing a risk assessment. The risk assessment should identify factors that could indicate a higher potential for conflicts of interest to exist. Such factors include organization size, reporting structure, or industry; regulatory considerations and geographical location of operations; analysis of key vendors, customers, and third-party relationships; and evaluation of duties that are more likely to be exposed to potential conflicts of interest. The risk assessment also should include any known board or employee relationships that could give rise to a conflict of interest. Additionally, the risk assessment should consider elements such as related employees, employees within the organization who share the same mailing address, employees who share the same mailing address as vendors, and any board members or employees in a position of influence who were previously employed by, or associated with, key vendors or customers of the organization. Each of these relationships could lead to various conflicts if not disclosed. From this initial analysis, the internal audit function should identify specific geographical locations using Transparency International's Corruption Perception Index—which ranks countries and territories based on how corrupt their public sector is perceived to be—and business functions (e.g., procurement, sales and marketing, and charitable giving/philanthropic) in which conflicts of interest may most likely exist based on the initial analysis.

UNDERSTANDING THE CONTROL ENVIRONMENT

Although the control environment sets the tone within the organization, conducting an initial risk assessment helps to provide an understanding of potential risks related to conflicts of interest based on the existing control environment. After the initial risk assessment has been completed, the next step is to develop an understanding of the control environment as it applies to conflict of interest, including any

PHOTO: OSTILL / SHUTTERSTOCK.COM

Guidance related to conflicts of interest may be embedded within the code of ethics policy.

policies and procedures for managing conflicts of interest within the organization. While the conflict of interest policy/process implemented likely will vary from organization to organization based on each organization's industry and other risk factors, there are several elements that should be considered from a control environment perspective. First, the internal auditor should evaluate whether a policy exists within the organization that defines *conflict of interest*, as well as the expectations of its employees related to conflicts of interest. In some organizations, guidance related to conflicts of interest may be embedded within the code of ethics policy or another applicable policy.

Regardless of where the conflict of interest policy is housed, it should:

- Emphasize the importance of identifying and resolving conflicts of interest, given the risk they represent to the organization.
- Clearly define the types of activities that are considered to be conflicts of interest.
- Identify the position/employee within the organization responsible for oversight of the conflict of interest process.
- Communicate the mechanisms for inquiring about, or reporting, any real or perceived conflicts of interest (both personal conflicts and any suspicions of conflicts of other employees).
- Communicate that all conflicts need to be reviewed and resolved in a manner that mitigates risk to the organization.

In addition, the auditor should determine whether there is a policy regarding acceptance of gifts and entertainment, including a definition of the types of gifts that are customary in nature, retail value thresholds, and requirements of a reporting and approval mechanism. In evaluating the

Anti-fraud controls are associated with reduced fraud losses and shorter fraud durations, according to the Association of Certified Fraud Examiners' 2014 Report to the Nation.

conflict of interest policy, the auditor should also determine whether the policy is reviewed and updated regularly. Given the pace that business risks, regulations, and technology are changing, it is critical that policies are periodically updated to reflect the current environment.

Following the evaluation of the existence and comprehensiveness of a conflict of interest policy, internal auditors should evaluate the frequency, timing, method, and documentation of completion of employee training on the policy. Training programs should provide employees a clear understanding of their roles and responsibilities related to conflict of interest. Further, in some industries or in some job-specific functions, it also may be necessary to have a conflict of interest disclosure form through which employees self-report annually any real or perceived conflicts of interest (see "Conflict of Interest Disclosure Form" on page 61). For positions in which an annual conflict of interest disclosure form is not completed, the auditor should consider whether the organization requires periodic acknowledgment of the conflict of interest policy from its employees. Combining the periodic conflict of interest declaration with the annual code of ethics acknowledgement or other similar existing process may increase the likelihood of participation.

Another tool to aid in determining organizational awareness of the conflict of interest policy is through evaluating whether information on the policy is posted in high-traffic areas throughout the organization, such as the company intranet or employee break rooms. This information also could be included in signage or online postings regarding the organization's whistleblower hotline or other key policies.

The internal auditor also should consider other controls in place throughout the organization that would aid in prevention, or early detection, of potential conflicts of interest. Examples of such controls include adequate segregation of duties, predetermined thresholds, and delegation of authority.

TESTS OF EFFECTIVENESS

An audit of the conflict of interest process also should include testing key elements of the policy to determine whether it is being followed. A secondary benefit of testing is that it may bring to light any policy items that need to be re-evaluated for ambiguity or confusion. Important items to consider in the testing process include determining adherence to the conflict of interest policy; evaluating potential interests in customers or suppliers; analyzing fees, entertainment, and employee reimbursements; and evaluating potential related-party transactions.

Adherence to Conflict of Interest Policy Because the policy provides the foundation for an organization's expectations related to conflict of interest, it is important to ensure that the policy is being followed. For example, if an annual acknowledgment of the conflict of interest policy is required, the auditor should test to determine whether the organization is actually obtaining acknowledgments from all of its employees. Further, for employees who are in positions that require annual completion of a conflict of interest form, the auditor should test whether the forms were completed timely by all employees. In addition, the internal auditor should review documentation of submissions and resolutions of a sample of all inquiries or concerns reported to the individual responsible for oversight of the policy. This step will ensure that the appropriate person reviewed each declared conflict and that mitigation strategies were implemented as applicable. Additional steps may include determining whether, and to what extent, any potential violations may have been reported via the whistleblower hotline or randomly interviewing employees to determine their understanding of the policy and steps they would need to take in the event of a concern.

Information on the conflict of interest policy should be posted in high-traffic areas throughout the organization.

Interest in Customers or Suppliers When auditing the conflict of interest process, internal auditors should consider testing significant business transactions to identify potential financial interests. While the specific approach, including transactions selected for testing, will vary among organizations based on industry, key business risks, and other factors, the objective remains the same—identifying transactions that could indicate a potential conflict of interest. Possible transaction types to consider for inclusion in the scope of testing include samples of critical or large dollar value contracts; material vendors, suppliers, and third-party payments; and strategic vendor relationships. Testing procedures should then be performed

TO COMMENT on this article, EMAIL the authors at laura.soileau@theiia.org

to determine whether established policies, procedures, and controls were followed throughout execution of the transactions. Examples include reviewing evidence that bids were obtained through a competitive bidding process when required by policy, low-cost vendors were selected or documentation exists detailing why the low-cost vendor was not selected, purchases were approved as per delegation of authority, appropriate documentation exists to support all purchases, and that performance quality of vendors was evaluated.

Additionally, some organizations require that all suppliers declare that they do not have a conflict of interest with the organization. Further, the suppliers often must acknowledge that if a conflict develops in the future, they will disclose the conflict at that time. One mechanism of continually reminding suppliers about the conflict of interest policy is to include a statement regarding the policy on all purchase orders. If such requirements are in place, the auditor should consider testing to evaluate compliance with the requirements, including evaluation of any conflicts identified through this process.

Evaluation of Fees, Entertainment, and Employee Reimbursements At small organizations, more widespread testing can be performed in this area due to the fact that there are fewer employees, but large organizations may consider testing fees and reimbursements of a sample of employees. The sample population should include those who are in positions of influence, employees who receive reimbursements above a certain threshold, and employees who have other risk factors. Upon determining the specific employees to be tested, testing procedures should be performed to evaluate whether appropriate documentation was maintained for all transactions, transactions were approved through the appropriate channels, and the organization was paying market rates for such expenses.

Evaluation of Related Parties/Financial Interests In June 2014, the U.S. Public Company Accounting Oversight Board (PCAOB) adopted Auditing Standard 18 regarding auditing related parties. This standard is intended to strengthen auditor performance requirements for identifying, assessing, and responding to the risks of material misstatement associated with a company's relationships and transactions with its related parties. The standard requires the external auditor to:

- Perform specific procedures to obtain an understanding of the company's relationships and transactions with its related parties, including the nature of the relationships and of the terms and business purposes (or the lack thereof) of transactions involving related parties.
- Evaluate whether the company has appropriately identified its related parties and relationships and all transactions among both. In making that evaluation, the auditor should test the accuracy and completeness of management's identification, while considering information gathered during the audit. If the auditor identifies information that indicates undisclosed relationships and transactions with a related party might exist, the auditor should perform additional procedures necessary to determine whether undisclosed relationships or transactions with such parties do in fact exist.
- Perform procedures specific to any undisclosed related-party transactions previously identified.
- Perform specific procedures regarding each related party transaction that is either required to be disclosed in the financial statements or determined to be a significant risk.
- Communicate to the audit committee the auditor's evaluation of the company's identification of, accounting for, and disclosure of its relationships and transactions with related parties, and other related significant matters arising from the audit.

Although organizations are not subject to PCAOB audit standards, the steps provide a solid foundation for both internal and external auditors to follow with respect to potential conflicts of interest associated with related-party transactions.

In addition to the specific tests of effectiveness, further areas also may be considered in the scope of testing, based on risk factors identified through the risk assessment process. Examples include assessment of potential conflicting business interests, analysis of gifts given or received by employees, and potential self-dealing.

Mechanisms should be in place to report significant conflicts of interest to executive management.

Organizations with **whistleblower** hotlines detect frauds **50%** more quickly than companies without, according to the Association of Certified Fraud Examiners' 2014 Report to the Nations.

CONFLICT OF INTEREST DISCLOSURE FORM

Elements often included in the conflict of interest disclosure form (specific elements vary, based on the organization, industry, and risks) include:

- Definition of *conflict of interest* and examples of types of conflicts.
- Acknowledgment that the employee has read and understands the conflicts of interest policy (may include a test to ensure understanding).
- Acknowledgment that the employee is familiar with the process to report conflict of interest.
- Acknowledgment that to the best of the employee's knowledge, there are no conflicts between the interests of the employee and his or her immediate family with the interests of the organization.
- Disclosure of any direct or indirect relationships of the employee and his or her immediate family members with key vendors, customers, those the organization is seeking to do business with, or others who could influence or appear to influence the employee in performing his or her duties and responsibilities objectively and promote the appearance of misconduct.
- Disclosure of any loans, significant financial interests, or other types of financial transactions that could influence or appear to influence the employee in performing his or her duties and responsibilities objectively and promote the appearance of misconduct.
- Disclosure of any gifts or benefits in excess of a defined amount that the employee or his or her immediate family members have received through the course of employment with the organization.
- Identification of methods to inquire about or report concerns of potential conflicts of interest.

REPORTING MECHANISM AND DISCIPLINARY PROCESS

The individual responsible for overseeing the conflict of interest process for the organization should investigate timely any potential conflicts that are reported. Such investigations should include determining whether an actual conflict exists, how any identified conflict was resolved, and any disciplinary actions taken (if necessary) within the organization. Mechanisms should be in place to report significant conflicts of interest to executive management and the board. Processes also should be in place to report noncompliance with completion of the conflict of interest acknowledgment and disclosure forms to appropriate management levels.

Whether potential conflicts of interest were identified through a self-disclosure form, brought to light by other employees, or identified through other mechanisms, the internal audit process should include an evaluation of the actions taken to remedy the conflicts identified. Next, the auditor should assess the responses to determine whether actions taken were appropriate based on the conflict of interest policy, including communication to all applicable parties within specified time frames and any other policy requirements.

In some cases, particularly for conflicts of interest that are voluntarily self-disclosed by employees, the conflict of interest may not be a specific violation of the terms of employment, but may necessitate awareness and limiting an employee's responsibility within a particular situation. One such example would be identifying another person to approve purchases with an organization that has ties to the employee.

Other disciplinary actions may be necessary for flagrant violations of the conflict of interest policy. Depending on the severity of the violation, disciplinary actions could range from a written warning in the employee's personnel file to termination of employment and, in some cases, criminal prosecution. This is a critical component of the conflict of interest process, in that if appropriate disciplinary actions are not taken, it may send a signal to employees that the conflict of interest policy is only casually regarded within the organization.

In the end, auditing the conflict of interest process can determine whether the process is meeting the organization's objectives, as well as reducing its operational, financial, and reputational risks. Ia

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

Governance Perspectives

BY MARK BRINKLEY

HOW TO FIND INDEPENDENCE

To fully embrace a behavior, the auditor must understand the rationale for the objective.

Opinions on internal auditor independence—what it is and how it is best achieved—are as varied as the factions of a political party, with many people weighing in with near rancorous commentary. Internal auditors debate the concepts of "Is it to whom we report?" Maybe it is "How we report." Some even dare submit that it is a state of mind.

To further demonstrate our passion, we create checklists to assess our independence. Checklists, however, provide security when there is no sincere mind-set for behavioral performance; basically, a checklist is false security. To fully embrace a behavior, we must understand the rationale for the objective. In this case, what is the purpose and drive for independence?

Interestingly, one definition of *independence* includes much about self-sufficiency, self-reliance, autonomy, freedom from control, and thinking or acting for oneself. There is a lot of "self" in the definition. To that end, internal auditors should start with ourselves as we seek to arrive at what independence means. Auditors should first look to IIA Standard 1100: Independence and Objectivity and its interpretation (see page 65).

The interpretation mentions a reporting relationship. Although this interpretation is more a recommendation than a hard-and-fast rule, internal auditors do like to drive the "independence through reporting structure" point home as a concrete representation of how things should be, based upon this standard. That said, we seem to lose sight of the thesis of the interpretation: "freedom from conditions that threaten the ability of the internal audit activity." This thesis specifically expresses "conditions," which include not only our reporting structure but how we conduct our work and our state of mind as we execute. How can we achieve true independence and be free from all impediments that threaten the audit activity, regardless of the functional organization chart? There are three key elements that truly represent independence:

Individual Objectivity The cardinal rule must be: The internal auditor is free from any conflict *or* perception of conflict. Perception is key. Basically, we can apply the concept that any reasonable outside view would conclude that internal audit individuals, teams, and management are fair and impartial. A breach in this construct of independence quickly destroys any work the auditor performs.

Integrity The first tenet of the integrity construct would be how the work is performed—meaning execution of work that garners trust and reliance upon the quality of the statements and opinions

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

IIA Audit Group Membership

Join. Save. Succeed.

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

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

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

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

The Institute of Internal Auditors

2015-1316_CX

stated. The auditor must not only understand the rule of the guideline operating as the basis of the audit test, but also what is intended by management or the board. This understanding requires a high degree of judgment and interpretation by the auditor. It is through the process of exercising exceptional audit judgment that integrity is demonstrated. Having integrity is paramount to ensuring internal audit is perceived as putting others' interests ahead of our own as we perform our work.

Due Care This concept must be a part of the independence conversation, for if we are not strong regarding self-awareness at each level—individual, engagement, and functional—our independence will be challenged. We must understand our core competencies and be willing to seek out others who complement our skills when conditions warrant. Continually improving our skills, recognizing when we need requisite experience or assistance, and ensuring our work product is consistently improving all support our exercise of due care.

The best contemporary example of these tenets is held in the WorldCom whistleblower story. In this example, the

INDEPENDENCE & OBJECTIVITY

Standard 1100: The internal audit activity must be independent, and internal auditors must be objective in performing their work.

Interpretation

Independence is the freedom from conditions that threaten the ability of the internal audit activity to carry out internal audit responsibilities in an unbiased manner. To achieve the degree of independence necessary to effectively carry out the responsibilities of the internal audit activity, the chief audit executive has direct and unrestricted access to senior management and the board. This can be achieved through a dual-reporting relationship. Threats to independence must be managed at the individual auditor, engagement, functional, and organizational levels.

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

consensus view companywide was that it was just a mistake made in the accounting entries. Even the Audit Committee chose to allow management to develop a white paper demonstrating the case. We know the ending well, the truth would eventually expose a multi-million dollar fraud. Cynthia Cooper is quoted as saying she moved from curiosity to discomfort to suspicion. It is precisely these "due care" and "integrity" elements that drove her—she possessed a certain state of mind. She did not ignore these as a basis of her individual objectivity. To be clear, Cooper supports a strong relationship with the audit committee and a reporting structure to demonstrate independence from management. However, the key takeaway from this example is the reporting relationship and even the lack of risk awareness of arguably all others in decision-making positions did not deter Cooper.

As demonstrated by Cooper, the three constructs of objectivity, integrity, and due care, considered together, provide a different view of independence than one of functional position within the organization. While the functional reporting is important, it has little relevance to individual objectivity, integrity, and due care. These elements are more about who we are, how we express our work, and how we can bring each into our conversation. Taken together, they provide guidance that independence is more the ability to render impartial and unbiased judgment than a reporting structure.

Further, we should consider how each of these tenets is not individually complacent, nor independent. What is individual objectivity if the individuals involved in the audit process have no integrity? The same considerations are present with due care and integrity—we can be well-versed in the functional process and audit theory but have little in the way of integrity. When any one of these concepts is lacking, our state of mind becomes imbalanced, leading one to conclude that independence is clearly and outwardly impaired.

Do not let these tenets lead you to a checklist. Each must become a part of your very being and become "living" as you do your work. Those you encounter will see the difference in your approach, possibly concluding that independence is a mind-set shown through specific and distinct behaviors. Ia

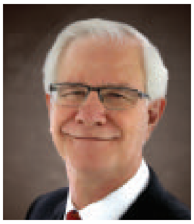
MARK BRINKLEY, CIA, CFSA, CRMA, *is director of Internal Audit for the Ewing Marion Kauffman Foundation in Kansas City, Mo.*

STATEMENT OF OWNERSHIP MANAGEMENT & CIRCULATION

Extent and Nature of Circulation	**Average No. Copies** (October 2014-August 2015)	**Actual No. Copies** (August 2015)
Total Number of Copies	85,102	85,794
Paid Circulation Mailed Outside-County Paid Subscription	59,660	59,701
Paid Distribution Outside the Mails Including Sales, Through Dealers and Carriers, Street vendors, Counter Sales, and Other Paid Distribution Outside USPS	24,035	24,613
Total Paid Distribution	83,695	84,314
Free or Nominal Rate Copies Mailed at Others Classes Through the USPS	379	315
Free or Nominal Rate Distribution Outside the Mail (*Carriers or other means*)	107	0
Total Free or Nominal Rate Distribution	486	315
Total Distribution	84,181	84,629
Copies Not Distributed	920	1,165
Total	85,101	85,794
Percent Paid	99.42%	99.63%
Paid Electronic Copies	41	49
Total Paid Print Distribution + Paid Electronic Copies	83,736	84,363
Total Print Distribution + Paid Electronic Copies	84,222	84,678
Percent Paid – Both Print & Electronic Copies	99.42%	99.63%

Publication Title: *Internal Auditor*
Publication Number: 0020-5745
Filing Date: 9/28/15
Issue Frequency: Bi-monthly
Number Issues Published Annually: 6
Mailing Address of Known Office of Publication: 247 Maitland Avenue, Altamonte Springs, FL 32701-4907
Address of Headquarters: The Institute of Internal Auditors, 247 Maitland Avenue, Altamonte Springs, FL 32701-4907
Contact Person: Gretchen Gorfine Telephone: 407-937-1232
Publisher: William Michalisin, COO, The Institute of Internal Auditors, 247 Maitland Avenue, Altamonte Springs, FL 32701-4907
Editor: Anne Millage, Editor-in-chief, The Institute of Internal Auditors, 247 Maitland Avenue, Altamonte Springs, FL 32701-4907
Managing Editor: David Salierno, The Institute of Internal Auditors, 247 Maitland Avenue, Altamonte Springs, FL 32701-4907
Owner: The Institute of Internal Auditors, Inc., 247 Maitland Avenue, Altamonte Springs, FL 32701-4907
Issue Date for Circulation Data: October 2014 - August 2015 / August 2015

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



BY J. MICHAEL JACKA

DREAM BIG

When we say we aspire to more as a profession, let's really set the bar higher.

Next year marks The IIA's 75th anniversary—a milestone definitely worth celebrating. And most would agree that one of The Institute's greatest achievements has been helping the profession evolve from the often-too-aptly-named bayoneters of the wounded to risk-based, future-focused, independent, and objective assurance providers. In the coming year we will hear a lot about the strides made in these areas.

Likewise, milestones like this provide an excellent opportunity to look forward, so we can also expect to hear a lot about the profession's future. I'm sure those prognostications will include refrains about the need for internal audit to be future-focused, incubators of talent, aligned with organizational goals, and partners to the business with a seat at the table.

These ambitions are all well and good—in fact, they represent the bedrock of our ability to add value. However, that's the problem. These are table stakes for today, not a vision of tomorrow.

It is time to want more. It is time to envision a future that does more than tweak our current situation. It is time for internal auditing to shed its risk-averse approaches and develop bold and ambitious goals reflecting the true value internal audit can provide.

We should be looking toward a time when a greater percentage of CEOs come from the CAE ranks. We should be working to get stronger regulatory backing for the profession. And we should be moving beyond having a seat at the table, aspiring to become the department to which CEOs immediately turn for advice. But ultimately, we should be setting a more audacious goal—we should be striving to work our way out of a job.

If we were doing our job—if we were helping strengthen control and risk structures; if we were educating people on the roles of governance, risk, and control; if our organizations were genuinely being improved by the work we do—wouldn't the result be a reduction in resources allocated to internal audit, and a reallocation to the other lines of defense? Shouldn't our ultimate goal be to enable the organization to rely on a strong control framework? Shouldn't this reduce the need for internal audit to watch every risk and control?

Unfortunately, the profession seems stuck in its old ways. As one example, far too many auditors continue to be enmeshed in work associated with the U.S. Sarbanes-Oxley Act of 2002. There is no proof of buy-in, no proof of increased understanding, and no proof that executives see a role beyond signing on the dotted line.

The 75th anniversary is an important milestone. And it is happening at a pivotal time of unprecedented challenges and opportunities. We have to want the profession to be much more than it is now. And, ironically, achieving more may be measured by becoming less. 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

Eye on Business

GETTING IT RIGHT

The CAEs of Delta Air Lines and Aflac discuss their approaches to hiring and retaining internal audit talent.

ALEXANDER STEPHANOUK, CIA, CRMA
Chief Audit Executive
Aflac Inc.

KIKO HARVEY, CRMA
Vice President/Chief Audit Executive
Delta Air Lines Inc.

What should colleges be teaching students to ensure they graduate with the skills they need to be successful internal auditors?

HARVEY It's really difficult to provide practical experience in a college setting, as each internal audit practice needs to be adapted to the risk environment of the company served. However, critical thinking skills, basic audit techniques—risk assessment, audit objectives, designing audit programs, and workpaper documentation—would be helpful to know. In addition, data analytics and report writing are important skills, along with verbal presentation, process flow diagrams, and negotiating skills. Finally, it is important to know The IIA's *International Standards for the Professional Practice of Internal Auditing.*

STEPHANOUK Data analytics should be taught to all business majors. Companies like Aflac are making a significant investment in tools to capture and analyze data. Our recruits need the capacity to understand those tools and how we can use them to solve problems and provide insight. Using data effectively requires a scientific process to answer creative questions. If our college recruits arrive with a data mind-set, they will already have experience in proposing and solving for hypotheses, which is in effect what we do with our internal audits.

What is your approach to recruiting new internal auditors?

STEPHANOUK Aflac's departmental philosophy is to promote from within when feasible and rotate experienced professionals into the business. So we must maintain an effective talent pipeline. To do that, we have selected some key schools for relationship-building to ensure we get the best possible recruits in terms of talent and cultural fit. Of course we are in competition with the Big 4 public accounting firms and many other companies, so we try to appeal to college recruits by supporting continuing education, providing flexibility in schedules, clear career paths, and opportunities for growth. We also try to have a continuous flow of new recruits so they have peers with whom they can interact and support. I'm sure our initial college recruits were somewhat intimidated as the youngest and least experienced people in the department, but now we have a group that is separated by months rather than decades.

HARVEY We typically hire experienced staff from public accounting firms because we like auditors to have some work experience—two to three busy seasons—under their belts before joining us. We have been successful attracting these strong candidates because Delta offers competitive compensation

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

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

and exceptional travel benefits. And, most importantly, internal audit in a complex industry such as ours is fascinating. Our team is never bored. Our hiring practices may change somewhat as we develop more of our own internal training programs geared to the newly graduated auditor.

Do the expectations of the younger generation of auditors differ from other generations?

HARVEY I'm not sure there is a significant difference. All auditors I've worked with are self-motivated, highly intelligent, well-prepared, professional, and curious. They work hard, are willing to work long hours—provided the work is meaningful and challenging—and are very efficient. The only difference in today's auditors from those of my generation is that they seem to be able to concentrate with numerous distractions around them. I've always found it difficult to focus without complete silence, so I admire their ability to multitask.

STEPHANOUK I have found the younger generation to be amazing. The people Aflac has recruited out of college have incredible creativity and passion for learning. Their ability to solve complex problems has exceeded my expectations. I've also noticed that their vast network has much more than just social value. They are able to reach out to peers in other organizations, former professors, and others they meet along the way to seek advice, which dramatically condenses the problem-solving cycle.

What steps do you take to help ensure you retain talented, new auditors?

STEPHANOUK Aflac tries to ensure all of our auditors see the value in each project they are assigned, and we encourage them to go beyond basic assurance and provide insight to management. This type of challenge gives them the opportunity to hit "home runs" and gives them more exposure to management. That combination of challenge and exposure seems to especially motivate our younger auditors. We also focus heavily on professional development through investment in training, supporting certifications, mentoring, and rotational opportunities. We just completed a training program that included courses on professional judgment, critical thinking, and root-cause analysis. Teaching those skills and then allowing our auditors to apply them in practice is highly motivating and contributes greatly to staff retention. Also, because we try to promote from within first, we are able to keep advancing our auditors through the talent pipeline in line with their general expectations.

HARVEY We keep the work challenging and make sure they are provided plenty of feedback. It's also helpful to be able to discuss a career path based on their interests. I'm not sure our timetables are always aligned, but it's important to continue to have these discussions.

Are there opportunities for mentoring at your organization?

HARVEY Our company has a formal mentoring program in place, but I also find that people will seek mentors through informal means. I find it's more common to have sponsors, rather than mentors, when you reach a higher level of leadership.

STEPHANOUK Aflac offers a formal mentoring program where anyone can seek a mentoring relationship, but I encourage people to network and build relationships with people they admire and let that relationship naturally evolve into one of mentoring. We also encourage all of our people to have mentoring relationships with people outside their reporting relationships.

What are other ways in which you help ensure new auditors benefit from, and contribute to, the organization's culture?

STEPHANOUK Aflac has a strong, positive culture of ethics, integrity, diversity, and work-life balance. We are a 17-time recipient of *Fortune's* 100 Best Places to Work recognition, and we have received Ethisphere's World's Most Ethical Companies designation every year since 2007. All new employees are oriented to our Aflac Way and given opportunities to participate in programs beyond our department. We encourage community involvement and following personal passions by giving time for community services and allowing flexibility in schedules. We also encourage our newer auditors to be ambassadors of our company and department in recruiting.

HARVEY Each company has its own unique culture. There are many ways our employees can get engaged in company activities and learn the culture. Being a large, diverse company provides the ability for our employees to get involved and take leadership positions outside of internal audit in numerous employee networks ranging from gender, culture, ethnicity, and socially oriented groups to sports teams and charitable activities. In addition, within internal audit, I think the work we do and the spirit in which our leaders accept and implement our recommendations helps our audit team members feel they are making a contribution to the overall improvement of company processes, policies, and activities. This really helps make a difference and keeps spirits high. Ia

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

BY JOHN A. HOWARD

A SIMPLE CONTROL

When it comes to recommending internal controls, a return to basics is often in order.

Internal controls, when designed well and executed consistently, are an essential part of achieving any set goals. But to be effective, controls must be selected with care and used judiciously. When internal auditors recommend new or enhanced controls, they need to do so with practical considerations in mind—especially cost. Yet auditors often tend to recommend the latest, greatest, and most robust measures, with little regard for the organization's ability to implement them. Practitioners need to resist this urge and, when appropriate, get back to the basics of internal control.

In many areas, tools that worked well in the past are abandoned for the most recent technology or developments, even though they do not necessarily represent an improvement. Consider home remedies for illness handed down through generations that are still just as effective, if not more so, than the latest prescriptions or over-the-counter medications. Internal auditors must take into account the financial and human resources of the organizations within which they work, just as a physician must consider the patient's means in deciding whether to prescribe a low-cost, generic medication over an expensive new drug.

The adage "keep it simple, stupid" should apply whenever recommending controls. As a first step, auditors should look to see whether existing controls can be adapted to cover any identified, unremediated risk. If no such controls exist, then they should recommend preventive controls, which are typically less costly than detective controls in the long run.

Segregation of duties falls within the keeping it simple principle, serving as a preventive control and typically costing little to implement and maintain. Yet perhaps due to its simplicity, auditors may overlook this tried and proven control. Moreover, segregation of duties issues are not restricted to instances where isolated individuals are performing incompatible functions, and internal auditors should not be blinkered into thinking these are the only situations where such issues are manifested. For example, a department of many people may be performing incompatible functions, such as an accounts payable department preparing checks and also maintaining responsibility for distributing those checks. Internal auditors must understand and be watchful for instances where segregation of duties is inadequate, whether it involves a whole department or a single employee.

For all organizations, especially smaller ones with limited human resources, internal auditors must take into account the feasibility of their control recommendations. That means avoiding recommendations that clients use a proverbial sledgehammer when a gentle tap would do. As you get ready to prescribe your next new control, be mindful of your biases, and keep it simple whenever possible. Ia

JOHN A. HOWARD, CIA, CPA, *is manager, SOX Compliance, at Cross Country Healthcare Inc. in Boca Raton, Fla.*

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