Ia
INTERNAL AUDITOR

OCTOBER 2017 INTERNALAUDITOR.ORG

COSO ERM: It's All About Strategy and Performance

Articulating Materiality

Knowing the Business Inside and Out

Control Self-assessments Address Repeat Findings

This year's Emerging Leaders are ambitious, poised to take on new challenges, and ready to lead.

ON THE RISE 2017

Ia
INTERNAL AUDITOR

OCTOBER 2017 VOLUME LXXIV: V

FEATURES

Introducing

Points of View by Pelletier

Insights and Innovations From an Insider

Premiering Monday, October 2, 2017!

Internal Auditor magazine is proud to feature this insightful and original blog. As a notable internal audit insider, Jim Pelletier, CIA, CGAP, vice president of Professional & Stakeholder Relations at The IIA, has taken, and kept, good notes over his career. His points are always well received, and now he's sharing them with you. We invite you to read Jim's blog at **InternalAuditor.org/jim-pelletier.**

READ ALL OF OUR BLOGS. Visit InternalAuditor.org.

Jim Pelletier

Vice President, Professional
& Stakeholder Relations
The IIA

Ia
INTERNAL AUDITOR

Ia
INTERNAL AUDITOR

OCTOBER 2017 VOLUME LXXIV: V

DEPARTMENTS

PRACTICES

INSIGHTS

ONLINE InternalAuditor.org

Build Your Brand Internal auditors can enhance their image and improve stakeholder relationships by following a sequence of steps aimed at improving the department's brand.

New Leaders Emerge In a series of video featurettes, this year's Emerging Leaders honorees share the secrets of their success.

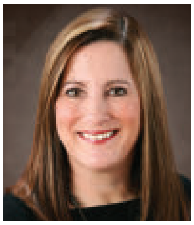
Aboard the Bribery Train Multinational organizations need strong anti-corruption practices to stay free of complex schemes. Fraud expert Art Stewart explains why.

Tech vs. Fraud Cybersecurity and digital forensic skills are in high demand for fraud fighters, the Association of Certified Fraud Examiners reports.

Find us on Facebook

Internal Auditor ISSN 0020-5745 is published in February, April, June, August, October, and December. Yearly subscription rates: $75 in the United States and Canada, and $99 outside North America. No refunds on cancellations. Editorial and advertising office: 1035 Greenwood Blvd., Suite 401, Lake Mary, FL, 32746, U.S.A. Copyright © 2017 The Institute of Internal Auditors Inc. Change of address notices and subscriptions should be directed to IIA Customer Service, +1-407-937-1111. Periodicals postage paid in Lake Mary, Fla., and additional offices. POSTMASTER: Please send form 3579 to: Internal Auditor, 1035 Greenwood Blvd., Suite 401, Lake Mary, FL, 32746, U.S.A. CANADA POST INTERNATIONAL: Publications Mail (Canadian Distribution) Sales Agreement number: 545880; GST registration number: R124590001. Opinions expressed in *Internal Auditor* may differ from policies and official statements of The Institute of Internal Auditors and its committees and from opinions endorsed by authors' employers or the editor of this journal. *Internal Auditor* does not attest to the originality of authors' content.

IMAGES: TOP, CHOMBOSAN / SHUTTERSTOCK.COM;
RIGHT, ALPHASPIRIT / SHUTTERSTOCK.COM



FROM EMERGING TO OUTSTANDING

For the fifth consecutive year, *Internal Auditor* is recognizing the rising leaders in the internal audit profession. The magazine's Emerging Leaders program was created in 2013 to not only highlight outstanding young internal audit professionals, but also to bring forth the next generation's voice within The IIA—a must-do as millennials are expected to comprise 50 percent of the workforce by 2020.

The program has been an overwhelming success. Since its debut, many of these leaders have gone on to contribute to the profession in a variety of ways. Their contributions enable The IIA to better determine what is important to the next generation and the tools they need to do their jobs, as well as share with previous generations the views and approaches of up-and-coming internal auditors.

Take, for example, Seth Peterson (@swpete85), one of our original Emerging Leaders. Seth was already a member of The IIA's Chapter Relations Committee when he was named an Emerging Leader in 2013. By 2016, he sat on The IIA's Audit Committee. Today, he is a member of The Institute's Global Finance Committee and vice chair–finance of the North American Board.

Seth also serves as the North American Board liaison to The IIA's Young Professionals Task Force. Among the priorities of this task force, which includes Emerging Leaders from 2015 and 2016, are contributing to articles and webinars, planning networking opportunities at IIA events, and providing insight to the North American Board related to attracting and serving young professionals.

Other Emerging Leaders are serving on IIA committees and participating in a variety of ways to advance the profession. Laura Soileau (@laurasoileau) was a member of the Publications Advisory Committee when she was named an Emerging Leader in 2014 and continues on the committee to this day. She also has been elected to the North American Board. Laura has served as a "Back to Basics" contributing editor, won an outstanding contributor award for an article she co-authored, and currently authors the InternalAuditor.org blog, "Solutions by Soileau."

The Emerging Leaders' continued participation in The IIA validates what we originally saw in them—their passion for, and willingness to give back to, the profession. We're proud to present our 2017 Emerging Leaders (see page 26). The future of the profession is indeed bright with these forward-looking, motivated, impressive individuals poised to take it to the next level.

Speaking of forward-looking, be sure to check out InternalAuditor.org's newest blog, "Points of View by Pelletier." Jim Pelletier (@JimLPelletier), The IIA's vice president, Professional and Stakeholder Relations, guides readers through innovative technologies, practices, and thinking for today's disruptive times.

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.

Ia
INTERNAL AUDITOR
Managing and Protecting Data
Tech Expectations of Today's Internal Auditor
Analytics and the Audit Function
New IIA Global Chairman on #PurposeServiceImpact
THE TECHNOLOGY ISSUE

Quality Reporting

Mike raised some good points about editing audit reports. He is spot on when the report is edited so much that the auditor's words are no longer his or her own. His three lessons boil down to open and honest communication between the auditor writing the report and upper management reviewing it. As an audit supervisor, I have made it a practice to keep auditors informed about what I edited in the report and why. In all of my edits, I include comments that provide feedback or questions for their consideration. I encourage the auditor to discuss the changes and edit my changes, if needed. In most cases, the auditor and I review the report together to allow for faster review, hands-on learning, and better communication about the report. Overall, communication is the key to ensuring that a quality report is issued, while keeping the auditor's voice intact.

FREDRICK LEE *comments on Mike Jacka's "It's Only One Word" ("The Mind of Jacka," August 2017).*

#PurposeServiceImpact

This was a great article that summarized vital concepts to the exercise of the internal audit profession. The #PurposeServiceImpact hashtag will definitely be part of my daily activities with my team. I am excited to read about increasing the level of conformance with the *International Standards for the Professional Practice of Internal Auditing* as part of initiatives during 2017–2018. Venezuela is excited to be a part of the Global IIA.

FABIOLA ALEJANDRA GALINDO VARG *comments on J. Michael Peppers' "#PurposeServiceImpact" (August 2017).*

Contributors of Value

In my experience working for big corporations or as a consultant, internal audit has never demonstrated its capability and competency adequately enough to gain audit committee confidence. Statutory auditors certify financial numbers, on which all stakeholders rely to an extent on internal audit observations on the robustness of systems and controls. For the audit committee, the role of statutory auditor is always bigger than internal audit.

Because internal audit's scope ranges from operations and finance reviews to verifying statutory compliance and even the robustness of enterprise risk management, the key concerns highlighted by internal audit appear to be too lengthy for the audit committee. If internal audit is not giving adequate coverage to all these areas, the first question stakeholders will ask is, "What was internal audit doing?"

Business managers earn profits and expand business for stakeholders, so they easily get away with excuses about working outside the rule book

Ia
INTERNAL AUDITOR
OCTOBER 2017
VOLUME LXXIV:V

EDITOR IN CHIEF
Anne Millage

MANAGING EDITOR
David Salierno

ASSOCIATE MANAGING EDITOR
Tim McCollum

SENIOR EDITOR
Shannon Steffee

ART DIRECTION
Yacinski Design, LLC

PRODUCTION MANAGER
Gretchen Gorfine

CONTRIBUTING EDITORS
Mark Brinkley, CIA, CFSA, CRMA
Wade Cassels, CIA, CCSA, CRMA, CFE
J. Michael Jacka, CIA, CPCU, CFE, CPA
Steve Mar, CFSA, CISA
Bryant Richards, CIA, CRMA
James Roth, PHD, CIA, CCSA, CRMA
Charlie Wright, CIA, CPA, CISA

EDITORIAL ADVISORY BOARD
Dennis Applegate, CIA, CPA, CMA, CFE
Lal Balkaran, CIA, CGA, FCIS, FCMA
Mark Brinkley, CIA, CFSA, CRMA
Robin Altia Brown
Adil Buhariwalla, CIA, CRMA, CFE, FCA
Wade Cassels, CIA, CCSA, CRMA, CFE
Daniel J. Clemens, CIA
Michael Cox, FIIA(NZ), AT
Dominic Daher, JD, LLM
Haylee Deniston, CPA
Kayla Flanders, CIA, CRMA
James Fox, CIA, CFE
Peter Francis, CIA
Michael Garvey, CIA
Nancy Haig, CIA, CFE, CCSA, CRMA
Daniel Helming, CIA, CPA
Karin L. Hill, CIA, CGAP, CRMA
J. Michael Jacka, CIA, CPCU, CFE, CPA
Gary Jordan, CIA, CRMA
Sandra Kasahara, CIA, CPA
Michael Levy, CIA, CRMA, CISA, CISSP
Merek Lipson, CIA
Thomas Luccock, CIA, CPA
Michael Marinaccio, CIA
Norman Marks, CPA, CRMA
Alyssa G. Martin, CPA
Dennis McGuffie, CPA
Stephen Minder, CIA
Jack Murray, Jr., CBA, CRP
Hans Nieuwlands, CIA, RA, CCSA, CGAP
Bryant Richards, CIA, CRMA
Jeffrey Ridley, CIA, FCIS, FIIA
Marshall Romney, PHD, CPA, CFE
James Roth, PHD, CIA, CCSA
Katherine Shamai, CIA, CA, CFE, CRMA
Debora Shelton, CIA, CRMA
Laura Soileau, CIA, CRMA
Jerry Strawser, PHD, CPA
Glenn Sumners, PHD, CIA, CPA, CRMA
Sonia Thomas, CRMA
Stephen Tiley, CIA
Robert Venczel, CIA, CRMA, CISA
Curtis Verschoor, CIA, CPA, CFE
David Weiss, CIA
Scott White, CIA, CFSA, CRMA
Benito Ybarra, CIA

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

IIA CHAIRMAN OF THE BOARD
J. Michael Peppers, CIA, QIAL, CRMA

PUBLISHED BY THE INSTITUTE OF INTERNAL AUDITORS INC.

CONTACT INFORMATION

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

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

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

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

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

to ensure continuity of business and its profitability. Internal audit has always been considered a function that works for stakeholders as a watchdog, even though business managers know in their hearts that timely appraising of critical areas and recommendations provided by internal audit have contributed to achievement of their own goals. We have been deliberating and voicing concern about the appropriate status of internal audit within any organization, but, sadly, it has not achieved its right status. Stakeholders have to drastically change their mindset and look at internal audit as one of the real contributors of value for their objectives.

LALIT DUA *comments on the Chambers on the Profession blog post, "Five Things the Audit Committee Is Still Reluctant to Say to Internal Audit."*

Generational Stereotypes

I've noticed this same trend [with generational stereotypes] perhaps over the past two years or so. I always thought of it as a discussion point and a topic for conversation—at a social gathering, not an audit meeting, and certainly not during an engagement interview—not a point of contention for hiring, not hiring, or the like.

I'd like to point out a few things that I've encountered about the subject: 1) These are indeed stereotypes (as Jacka points out), and I find I am more in keeping with pieces of the other generations than I am with my own, as I suspect is true for everyone else; 2) the years that delineate one generation from the next seem to be rather elastic (perhaps to support the author's statistics or metrics); and 3) using this as a basis of hiring or not hiring can easily lead to age discrimination action.

CMD047 *comments on the From the Mind of Jacka blog post, "Millennials, Xers, and Boomers, Oh My!"*

Disciplined Execution

Happy to hear everyone at IIA headquarters is OK—but you must be exhausted. You also show that a good risk assessment depends on a disciplined execution when things actually start to escalate. Looks like you have that covered.

KERI ROGERS *comments on the Chambers on the Profession blog post, "My Personal Risk Managment Journey Through Hurricane Irma."*

MORE
VISIT InternalAuditor.org for the latest blogs.

The high price of embezzlement... Firms get mixed cybersecurity grades... Adding value with integrated reporting... Analytics' independence impact.

Update

IOT HELP WANTED

A lack of Internet of Things knowledge – and skills – leaves businesses struggling to recruit talent.

Sixty-eight percent of Internet of Things (IoT) professionals have difficulty hiring people with IoT skills, according to a report commissioned by London-based Canonical, the developer of IoT operating system Ubuntu Core. Hardest to hire are employees with big data and analytics knowledge (35 percent)—critical to gathering, analyzing, and monetizing the huge amount of data produced by IoT devices—which is also the most important skill for IoT experts (75 percent).

Other hard-to-find IoT skills are knowledge of embedded software development (33 percent) and embedded electronics (32 percent), IT security (31 percent), and understanding of artificial intelligence (30 percent), according to the Defining IoT Business Models report. Independent industry publication *IoT Now* surveyed more than 360 IoT professionals, developers, and vendors from around the world.

"When it comes to the IoT, the business community is still overcoming a significant skills gap," Mike Bell, executive vice president of IoT and Devices at Canonical, explains. "Many businesses are concerned by their own lack of knowledge

FUNDING SECURITY

Most U.S. health-care organizations budget specifically for cybersecurity. Among them:

40% allocate **1%** to **2%** of the organization's budget

32% allocate **3%** to **6%**

17% allocate **7%** to **10%**

11% allocate more than **10%**

Source: 2017 HIMSS Cybersecurity Survey

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

IMAGES: TOP, CHOMBOSAN / SHUTTERSTOCK.COM

and skills within the IoT market, and many business leaders are finding themselves running headfirst into a set of technology and business challenges that they do not yet fully understand."

In a rapidly evolving industry such as IoT, it is difficult to see more than a few years into the future, the report notes. Organizations are better off identifying the skills required and then determining whether those skills are best outsourced for the short term, which has the benefit of bringing in IoT experts who can share knowledge throughout the business.

Bell says businesses must be agile when it comes to deciding on the right people, skills, and team to take them forward. "What is decided upon today is unlikely to remain the same in even one or two years, so constantly evaluating what change is needed and being able to execute this quickly is a must," he advises. **–S. STEFFEE**

50%

OF BOARDS GLOBALLY HAVE CULTURE AS A STANDING ITEM ON THEIR AGENDA.

71%

ARE ESTABLISHING INTERNAL CONTROLS THAT ADDRESS CULTURE AND EMPLOYEE BEHAVIOR.

"What's undeniable is that around the world, the issue of corporate culture is gaining increasing regulatory attention as a foundation of good governance," says Harish HV, partner at Grant Thornton India. "As a result, the issue has arguably never been as high up the business agenda as it is today."

Source: Grant Thornton, Beyond Compliance: The Building Blocks of a Strong Corporate Culture

EMBEZZLEMENT'S ENDURING COST

Small businesses pay a high price for long-term thefts.

Nearly one-fourth of U.S. embezzlement cases cost businesses more than $1 million, the 2017 Hiscox Embezzlement Study reports. Such crimes cost organizations median losses of $319,000.

More than half of employee fraud cases in U.S. federal courts in 2016 occurred in small companies, the study reports. Such breaches of trust by executives and employees can impact businesses significantly, according to Doug Karpp, crime and fidelity product head at Hiscox, a New York-based international specialist insurer. "Business owners and executives need to make the shift from blind trust to intelligent trust to ensure they are able to spot and prevent employee theft," he cautions.

Twenty-nine percent of embezzlement schemes had continued for five years or more, the study notes. Schemes lasting that long have average losses of $2.2 million. **–T. MCCOLLUM**

SEC ISSUES CYBER REPORT CARD

Financial firms are more prepared, but need to improve policies and plans.

The U.S. Securities and Exchange Commission (SEC) has offered a mixed report on the status of cybersecurity practices in the financial services industry. Detailing its survey of 75 regulated entities, the SEC Office of Compliance Inspections and Examinations (OCIE) National Exam Program Risk Alert provides observations of both improvements and problems.

Since its last survey, published in 2016, the OCIE points to an overall improvement in surveyed firms' awareness of cyber risks, as well as their implementation of certain cybersecurity practices. The office cites nearly all firms' maintenance of written cybersecurity policies and procedures aimed at protecting customer and shareholder data, and it notes

IMAGES: TOP, ANTONINA TSYGANKO / SHUTTERSTOCK.COM; LEFT, BIORAVEN / SHUTTERSTOCK.COM

that most firms conducted periodic risk assessments of critical systems to identify cybersecurity threats. All surveyed organizations used some kind of tool to prevent, detect, and monitor for data loss related to personally identifiable information.

Among areas for improvement, the OCIE cites many firms' use of only general guidance in their cybersecurity policies and procedures, with limited examples of safeguards for employees to consider. Moreover, the office points to a lack of adherence to, or enforcement of, policies and procedures, and failure to align with them in actual practice. It also notes that firms did not appear to perform system maintenance adequately, including critical software updates to address vulnerabilities. Some firms lacked clear plans for data breach incidents.

The OCIE lists several best practices observed during its examinations that could help organizations bolster their cybersecurity programs. Surveyed firms with robust cybersecurity protections, for example, maintained a complete inventory of data, information, and vendors, as well as classifications of accompanying risks. These firms also kept detailed cybersecurity instructions for penetration testing, security monitoring, and system auditing, and they maintained prescriptive schedules for testing data integrity and vulnerabilities. – **D. SALIERNO**

<IR> MAKES PROGRESS

Integrated reporting is an area where internal auditors can add value, International Integrated Reporting Council CEO Richard Howitt says.

As integrated reporting <IR> gains traction globally, what role can internal auditors play? Internal audit professionals' expertise puts them in a prime position to provide guidance to management on ways to protect and create value. The role of internal auditors is becoming more strategic as they identify key risks and provide assurance over increasingly broad value drivers. Internal auditors are key to effective integrated thinking, already having a sound understanding of the business and close relationships with the key players in the reporting process. The IIA has been a driving force behind <IR>.

However, <IR> is not yet well known enough in the U.S. There are big advocates of <IR> within the U.S. – General Electric, PepsiCo, JLL, and Prudential Financial are among the 25 organizations producing integrated reports. The largest U.S. public pension fund, CalPERS, has called on boards to provide an integrated report, and Black Rock CEO Larry Fink has called on businesses to set out a strategic framework for long-term value creation.

THE DOWNSIDE OF ANALYTICS

Data analysis technology could negatively impact internal audit independence.

Despite its benefits, data analytics can impact the quality and independence of internal audit's work, an Institute of Chartered Accountants in England and Wales (ICAEW) report warns. Risks include inaccurate or misleading results, misuse of data, independence conflicts, and data privacy and security, according to Internal Audit in the Age of Data Analytics.

"Internal auditors should focus on effective analysis of better data and strengthen their internal audit governance framework to cover emerging data analytics-related risks," the report advises.

That framework should include strong testing and quality assurance procedures to address issues with poor data quality, incorrect coding, and poor presentations that can lead audit clients to mistrust audit findings. The report also advises internal auditors to consider the disruptive influence analytics could

have on its client relationships and seek a collaborative approach that defines responsibilities for data sourcing, access, and quality.

To address data security, the report recommends internal auditors update their workpaper policies to define what data can be requested, where it will be stored, who can access it, how it can be accessed, and how long it may be retained. – **T. MCCOLLUM**

PHOTO: RIGHT, PESHKOVA / SHUTTERSTOCK.COM

BY LAL BALKARAN EDITED BY JAMES ROTH + WADE CASSELS

FOCUS ON THE THREE E'S

Embedding value-for-money auditing in work processes can ensure economy, effectiveness, and efficiency are achieved.

Although developed in and long associated with the public sector, the concept of value-for-money (VFM) auditing is finding increasing interest and application in the private sector. These organizations realize the true power and range of value VFM audits generate. Understanding this approach can help position internal auditors to exceed stakeholders' expectations. For example, VFM audits can enable resources to be acquired at optimal cost without jeopardizing quality and performance, unearth inefficiencies, and identify ineffective operations. Along the way, it also can help identify irregularities or potential indicators of fraud — all culminating in business improvements.

VFM auditing is embodied in Standard 2100: Nature of Work, which states, "The internal audit activity must evaluate and contribute to the improvement of the organization's governance, risk management, and control processes using a systematic, disciplined, and risk-based approach. Internal audit credibility and value are enhanced when auditors are proactive and their evaluations offer new insights and consider future impact."

Conforming to this standard requires a thorough understanding of the risks, governance structures, and control activities associated with improving business operations. This leads to assessing the acquisition of resources, evaluating business functions, and maximizing the achievement of goals — the very foundation of VFM audits. This foundation focuses on the three E's: economy, efficiency, and effectiveness.

The VFM auditor asks: Are the right operations being performed to achieve the objectives of the unit (effectiveness) in the right way (efficiency) at an appropriate cost (economical use of resources or economy)? Answering such questions involves assessing an appropriate range of performance measurement criteria. For instance, if procurement is not acquiring goods and services at the right prices in the right amount and on schedule, then it is not effective because it is not achieving its goals. VFM audits can be applied to any business function such as finance, procurement, human resources, and marketing, as well as to any industry.

When performing a VFM audit, the auditor must possess a multitude of skills; be multidisciplined; let go of the financial statement audit mindset; be able to think outside of the box; ask challenging questions; be persistent and question the validity of information; and be able to work as a team player with subject matter experts, accountants, IT specialists, and management.

SEND BACK TO BASICS ARTICLE IDEAS to James Roth at jamesroth@audittrends.com

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

The Foundation

Economy alludes to the cost of resources (i.e., minimizing the cost of resources used for an activity without compromising quality). For example, if components "A" and "B" can equally be used and cost $20 and $30 each, respectively, to make product "C," then purchasing the cheaper component "A" is the better option. Also, when copying a report for distribution, is the business unit using an expensive copying paper (70 cents/sheet) versus a cheaper (3 cents/sheet) paper to produce the same report? This review also could expose fraud if it is revealed there is collusion between the paper supplier and an employee to use more expensive paper. Do you send a report by mail, which incurs postage or courier costs, when it can be emailed at no cost? Other factors to consider when reviewing economy are determining that sound business practices are carried out, an optimal staff level is in place, excess resources are not on hand, and cheaper equipment is used where required.

Efficiency pertains to the methods of operations and include identifying slack, waste, redundancy, and duplication of effort; determining inappropriate use of operating procedures; identifying inefficient systems and procedures; and ensuring maximum outputs from inputs. The types of questions to ask during this aspect are:

- Is activity "A" necessary?
- Can two machines be used instead of one?
- Can activity "B" be completed in five minutes instead of 10?
- Is activity "C" a duplicate of activity "A"?
- Department "A" produces 120 widgets against a plan of 100 indicating 120 percent efficiency, but department "B's" efficiency is 80 percent—producing 80 against a target of 100. Is this because of staff training issues or something else?

Effectiveness measures the extent to which the objectives of an activity are achieved. It asks questions such as:

- Are the right operations being performed?
- Are objectives achieved?
- Are these achieved objectives having a positive impact?
- What factors exist to inhibit the satisfactory performance of a unit in achieving its objectives?

VFM audits add value to an organization in each of its three phases. Identifying and costing inefficient activities such as waste and duplication of effort, and validating that desired goals were achieved at minimal cost and with maximum efficiency, can have a dramatic and long-lasting impact on an organization.

Key Benefits

Understanding and carrying out a VFM audit can provide tremendous benefits to stakeholders in an organization by unearthing audit findings to aid management to discharge its mandate and allocate resources optimally. Within this context, a VFM audit:

- Focuses on organizational and management performance.
- Facilitates and promotes improved strategic and operational decision-making.
- Assists management by identifying and promoting better management practices.
- Clarifies management responsibility and leads to better accountability.
- Enhances efficiency in the acquisition of resources.
- Allows assessments over the achievement of objectives.
- Identifies performance gaps by comparing input resources and expected outcome as well as the actual outcome.

Ultimately, VFM audit findings must stand on their own to add value to the organization.

VFM audits can unleash significant benefits to the organization.

A Powerful Tool

In any organization, there is an emphasis on getting maximum output from resources expended. An evaluation of all business functions is needed to ensure minimum- and lowest-cost resources are used without compromising the quality of output, inefficient activities are identified and eliminated, maximum outputs are obtained from minimal inputs, and objectives are realized to collectively achieve the greatest returns. VFM audits can be used to accomplish these tasks, unleashing significant benefits to the organization's governance, risk management, and control environments. VFM auditors should be an integral part of the audit effort, as reflected in The IIA's Core Principles for the Professional Practice of Internal Auditing's emphasis on promoting organizational improvement. Ia

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

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

BY BRAD BARTON + SAJAY RAI   EDITED BY STEVE MAR

WHO SHOULD AUDIT THE CONNECTED CAR?

Today's high-tech vehicles pose complex risks beyond the driver's control.

Connected cars that alert drivers to potential dangers or even automatically brake to avoid them promise greater automobile safety and efficiency. But the risks these advanced vehicles pose shift dramatically from driver attention and road hazards to cyber threats and the integrity of vehicle control systems. This threat was demonstrated when researchers were able to remotely take control of environmental, entertainment, and engine systems on a 2014 Jeep Cherokee.

Assessing related risks and controls is similar to other technology development initiatives. Internal auditors for automakers, equipment manufacturers, and business and government customers should learn the basics about connected cars and what can be done to address their risks.

Internal Connections

By definition, connected cars are linked to internal and external systems and services. Inside the vehicle, there's the Controller Area Network (CAN) bus that links internal micro-devices such as the engine control unit, transmission, braking, and diagnostic systems to various monitoring and control systems. This structure was originally developed in the early 1980s to accommodate the growing number of connected components while reducing the amount of wiring needed to connect onboard components. CAN relies on a serial bus protocol for message transport, fault/error detection, timing, etc. Because the CAN protocol does not support security, security must be designed into devices connected to the bus. As such, a security review should be part of any audit of devices connected to the CAN bus.

Also internal to the vehicle are physical ports for diagnostic and peripheral connections. On-board diagnostics (OBD) is a physical connection present in all vehicles produced since the early 2000s. OBD provides a standard connection for service technicians to attach diagnostic equipment and read status and error code information generated by sensors on the vehicle. OBD's direct access to the vehicle's internal sensors and control devices could make this connection susceptible to exploit.

Another risk is the Universal Serial Bus (USB) connectors that are common on many entertainment systems found in newer vehicles. These interfaces not only support streaming audio for entertainment, but they also can be used to update engine and system controls software. Given reports of how USB ports can be compromised, auditors should consider related risks in their connected car program.

External Connections

Moving on to external connections, the automotive industry has been developing wireless communications

SEND ITAUDIT ARTICLE IDEAS to Steve Mar at steve_mar2003@msn.com called vehicle to x (V2x) that allow vehicles to talk to each other and to roadway infrastructure. Here, the connections are established on the fly to allow for exchange of data relating to positioning, traffic signals, and on-the-road services. Variants on the V2x nomenclature include vehicle to vehicle, vehicle to infrastructure, and vehicle to pedestrian. Each variant sets up a wireless connection to accommodate the services, entertainment, or vehicle support. Threats to V2x connections include malicious attempts to communicate false hazard information and the privacy of information broadcast from car to car.

Other wireless communications that can support vehicle connections such as Bluetooth, cellular, and Wi-Fi have well-documented weaknesses. What differentiates them when incorporated into vehicles is their ability to interface with vehicle controls and safety functions. The risks increase when wireless communications are used to update vehicle control software, perform system diagnostics, or change performance and safety settings. One of the most important security-related questions is whether operating and safety systems within the vehicle are connected or isolated from these external communication channels. If they are not isolated, robust authentication systems should be in place to ensure that only authorized updates and signals can be sent to the vehicle.

Auditing Cars

Auditors who are assessing risk and testing appropriate mitigation processes should begin by examining the environment in which the connected car software is designed and written. Here, traditional controls should be in place, including perimeter security, strong authentication, threat detection, and appropriate response processes. All the necessary controls for maintaining a secure development environment are well-known, so the auditor should verify their presence and operating effectiveness. A connected car audit program should include this type of security review as the starting point.

For automakers and technology vendors, a connected car audit program must examine the software development processes to ensure there is appropriate attention paid to security throughout the design and testing steps. Although relatively new to the automotive industry, secure software development is a mature practice in adjacent industries. Fundamental to good development practices are steps to ensure appropriate

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

risk assessment, security design reviews, testing, authentication, and privacy. Risk assessment should be based on the fundamentals of confidentiality, integrity, and availability. Across all three risk areas, unique considerations arise when communicating to and from a moving vehicle. The Automotive Information Sharing and Analysis Center's Automotive Cybersecurity Best Practices guide summarizes security expectations and can be the core of a connected car audit program.

For auto buyers, such as businesses and government agencies operating auto fleets, internal audit can contribute by advising the organization on spelling out expectations in requests for proposals or purchasing documents. Examples of such expectations may be included in future U.S. government guidelines for purchasing connected devices.

Finally, privacy issues are a growing concern worldwide. Auditors should address how privacy compliance will be incorporated into the design and operation of vehicle systems. This includes data stored and analyzed in a remote cloud or data processing center. Auditors should examine practices for the collection and use of personal information. The Alliance of Automobile Manufacturers' Privacy Principles for Vehicle Technologies and Services explains the reasons for collecting vehicle operating data, and addresses fundamental considerations for maintaining consumer confidence in its transparency, appropriate use, retention, and accountability. The principles can be a good guide for planning a privacy audit.

Driving Awareness and Response

System development and privacy issues are among many reasons that internal auditors should expand their audit scope to encompass connected vehicles. Vehicle advancements that rely on outside connections are already available and expected to be widespread soon. In the best-case situations, the audit team will only need to confirm enterprise awareness and appropriate response to these risks. But in the other cases, audit can be the spark that initiates necessary actions to recognize and mitigate risks posed by this technology. Ia

BRAD BARTON, CISA, *is chief operations, risk, and compliance officer of Securely Yours LLC in Bloomfield Hills, Mich.*

SAJAY RAI, CPA, CISSP, CISM, *is president and CEO of Securely Yours LLC.*

Risk Watch

BY SEAN LYONS EDITED BY CHARLIE WRIGHT

CORPORATE DEFENSE

Protecting the organization requires integrating multiple disciplines into a single defense framework.

The delivery of sustainable stakeholder value in the 21st century requires internal auditors to focus on both value creation (offense) and value preservation (defense). While internal audit's focus on value creation has been increasing recently, many stakeholders still perceive its greatest contribution to be value preservation. Preserving value involves safeguarding against potential risks, thereby enabling the achievement of short-, medium-, and long-term objectives.

The value preservation imperative represents an organization's obligation to demonstrate that it is taking adequate steps to defend against value erosion, reduction, or destruction. Internal audit needs to be mindful of how its organization is fulfilling this obligation. By viewing risk through the lens of corporate defense, auditors have an alternative way to think about managing risks and protecting value.

The Defense Program

Corporate defense is synonymous with value preservation. A corporate defense program represents an organization's collective program for self-defense. A comprehensive corporate defense program requires a multidisciplinary approach that involves aligning, coordinating, and integrating eight distinct disciplines: governance, risk, compliance, intelligence, security, resilience, controls, and assurance (see "The Elements of Corporate Defense" on page 21).

As internal audit develops its risk assessments and audit plans, it should evaluate each of these components to determine whether they are incorporated into the organization's corporate defense framework and to assess whether they are being managed appropriately. Auditors need to fully appreciate the positive contribution each of these components makes both individually and collectively. Effective corporate defense requires a clear understanding of the continuous interaction, interconnections, and critical interdependencies that exist among these components. These complimentary disciplines continuously impact one another in today's complex organizations. In fact, the symbiotic nature of their relationships means that each contributes to, and receives from, each of the other components.

As organizations have developed these unique functions and disciplines, the boundaries between these components have become blurred. Therefore, it is difficult to determine where one component ends and another begins. Each component provides a different but essential perspective on dealing with risks. For example, viewing any issue through a *risk-centric* lens will produce a different perspective than when viewing the same issue through a *compliance-centric* lens.

SEND RISK WATCH ARTICLE IDEAS to Charlie Wright at charliewright.audit@gmail.com

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

THE ELEMENTS OF CORPORATE DEFENSE

A comprehensive corporate defense program includes these interrelated elements.

- **Governance:** How the organization is directed and managed, all the way from the boardroom to the front lines.
- **Risk:** How the organization identifies, measures, and manages the risks to which it is exposed.
- **Compliance:** How the organization ensures that its activities conform with all relevant mandatory and voluntary requirements.
- **Intelligence:** How the organization ensures that it gets the right information, for the right purpose, in the right format, to the right person, in the right place, at the right time.
- **Security:** How the organization ensures that it protects critical assets such as its people, information, technology, and facilities from threats.
- **Resilience:** How the organization ensures that it has the capacity to withstand, rebound from, or recover from the direct and indirect consequences of a shock, disturbance, or disruption.
- **Controls:** How the organization ensures that it has taken appropriate actions to address risk and help make certain that the organization's objectives will be achieved.
- **Assurance:** The system in place to provide a degree of confidence or level of comfort to the stakeholders that everything is operating satisfactorily.

By considering these many different perspectives, internal audit can develop a more holistic view of any issue and provide management with insight to help it avoid potential blind spots. Cross-referencing each of these specialist disciplines can help provide the organization with a robust system of checks and balances and help ensure that each of these disciplines becomes ingrained into day-to-day activities.

The Risk Component

Organizations naturally face a variety of different risks in the course of their business, and therefore they need to have an adequate system in place to manage risk at strategic, tactical, and operational levels. Enterprise risk management (ERM) frameworks such as The Committee of Sponsoring Organizations of the Treadway Commission's (COSO's) *Enterprise Risk Management–Integrating With Strategy and Performance* and ISO 31000 can help provide a system to organize standard risk management activities to ensure that the risk component is addressed adequately within the corporate defense program (see "COSO ERM: Getting Risk Management Right" on page 38).

Internal auditors, however, need to examine how the risk component relates to the other critical corporate defense components, particularly such issues as governance risk, compliance risk, intelligence risk, security risk, resilience risk, control risk, and assurance risk. Conversely, internal auditors also should consider how these other components relate to the risk component—specifically, risk governance, risk compliance, risk intelligence, risk security, risk resilience, risk controls, and risk assurance. Such cross-referencing represents the essence of a robust corporate defense program.

Internal Audit's Risk Assurance Role

IIA Standard 2120: Risk Management states, "The internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes." The standard goes on to say, "Risk management processes are monitored through ongoing management activities, separate evaluations, or both." Ongoing management activities are represented by the eight components of the corporate defense model.

As the organization's primary provider of independent assurance, internal audit must consider the effectiveness of each risk component in its totality to provide comprehensive risk assurance at strategic, tactical, and operational levels. This involves reviewing, assessing, and reporting on the effectiveness of a complicated, highly interrelated risk environment all the way from the boardroom to the front lines of the organization. Evaluating the organization through the lens of the eight critical components of the corporate defense model provides an alternative perspective to both COSO ERM and ISO 31000.

The requirement to provide comprehensive risk assurance may be one of the more serious challenges the internal audit profession faces. In this regard, internal auditors should begin by determining whether their organization has a formal corporate defense strategy in place. They also should report on the extent to which the organization has established a structured and integrated corporate defense framework. Moreover, auditors should review the current maturity level of each of the corporate defense components. Ia

SEAN LYONS *is the author of* Corporate Defense and the Value Preservation Imperative: Bulletproof Your Corporate Defense Program *(CRC Press).*

Fraud Findings

BY JAMES CARROLL EDITED BY BRYANT RICHARDS

THE PILFERING PARTNER

Taking advantage of trust and limited oversight, a business partner uses the company as a piggy bank for personal expenses.

Mike Billings of The Building Co. (TBC), a building contractor with $8 million in annual revenue, became concerned about the activities of his 50/50 business partner, Steve Grey. Grey had not prepared certain internal financial documents, including a statement of partner draws for the current year and standard financial statements, which Billings had requested months earlier. Based on his concerns, Billings conducted an initial review by analyzing selected disbursement transactions and identified multiple transactions executed by Grey to benefit his other businesses, including one for $300,000.

Shortly after Billings established TBC, he brought Grey in as an equal partner based on their prior work history and Grey's strong sales background. Although neither partner ever signed a legal partnership operating agreement, Billings acted as president and the only named officer, while Grey held the title of vice president in filed tax documents.

Each partner drew a salary, and an informal agreement between the partners allowed each of them to pass certain agreed-upon personal expenses through TBC as distributions. Based on the agreement, the partner with the lower amount of distributions at year-end would receive a cash distribution to equalize distributions between the partners.

While Billings focused on expanding the business, running projects that he sold, and developing TBC's business strategy, Grey's responsibilities included tracking costs and revenues for his projects, day-to-day general office operations, marketing and advertising, and maintaining the books and records. Although Grey had no accounting or other education related to handling business finances, Billings trusted him fully.

After the initial analysis, Billings contacted counsel and forensic accountants to conduct an investigation. Counsel directed the investigation to ensure privilege was maintained. The forensic accountants obtained forensic images and performed a forensic analysis of all of Grey's computers and business cell phones. In addition, they analyzed all relevant financial documents, including corporate and personal credit card statements related to Grey's activity. The investigation focused on:

- Extracting all accounting and financial data from the accounting software for the period under investigation.
- Obtaining all relevant contracts and supporting documentation.
- Leveraging Billings' knowledge of Grey's other businesses, his familiarity with TBC vendors likely used based on home improvements Grey had

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

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

completed, and his understanding of credit card charges that were not related to TBC's business.
- Interviewing TBC employees to understand internal controls and address specific topics related to the investigation.
- Communicating with management frequently to keep all stakeholders abreast of evolving issues.

Investigators determined that over a three-year period, Grey embezzled more than $450,000 to support his excessive lifestyle, which included gambling, and frequent and expensive trips to strip clubs that allegedly also included prostitution.

As part of his scheme, Grey used his corporate credit card to incur a portion of those personal expenses and had TBC pay those charges without Billings' knowledge. Those charges included taking himself and other TBC employees on gambling trips and spending extravagantly at restaurants and strip clubs. Grey recorded those transactions as "client/customer entertainment" in various general ledger accounts. He would then exclude these transactions from the shareholder distribution reports he generated.

Additionally, Grey executed two schemes to pay off his personal credit card charges. He would submit and approve his own expense report, and then issue himself a check from TBC (which he also signed) or he would issue a direct payment from TBC to his personal credit card company. The identification of improperly deducted nonbusiness expenses led to additional technical accounting and tax issues that required resolution.

Grey also provided a bridge loan to a TBC employee buying a house. During a discussion with the individual who received the loan, he stated that Grey charged him $15,000 in interest for the 30-day loan, which Grey kept. Grey returned $250,000 of the $300,000 bridge loan to TBC.

When examining TBC's internal controls and relevant financial information, the forensic accountants determined that Grey exerted full control over the financial processes and information at TBC and was able to manipulate financial information provided to Billings and stakeholders. Grey altered his project profit reports to exclude nonbusiness transactions he posted against the project in the general ledger either just before or just after a project's completion. Project reports clearly showed additional costs being added to Grey's projects at, or near the time of, job completion.

Grey also manipulated TBC's general ledger by mischaracterizing and falsifying descriptions for personal transactions, such as upgrades to his personal residence and new appliance purchases. This was determined by vouching general ledger transactions to reliable/competent supporting documentation or, in some instances, missing supporting documentation indicating the transaction was valid.

He also disguised nonbusiness transactions by identifying them as charge-backs on a project profit report or classifying a personal vendor payment as a subcontractor expense. In many instances, he recorded the false charge-back transactions in the subcontractor expense category because this represented the largest expenditure for TBC, and Billings never reviewed this account in detail.

In addition to the lack of segregation of duties related to the financials, investigators also discovered that Grey signed most checks and interacted with, and supervised, the outside part-time bookkeeper, who recorded transactions as directed by Grey. He also controlled the interaction with the tax accountant and provided all related financial information without Billings' knowledge. Unfortunately, due to TBC's deficient IT infrastructure, its server did not back up the accounting system, so all accounting-related information before 2012 was lost.

Ultimately, Billings bought Grey out of the business for a price that factored in the embezzled funds, but elected not to press charges to avoid the negative public relations impact and the potential for lost customers. TBC, Billings, and Grey had to refile three years of business and personal tax returns and had to pay additional federal taxes and penalties.

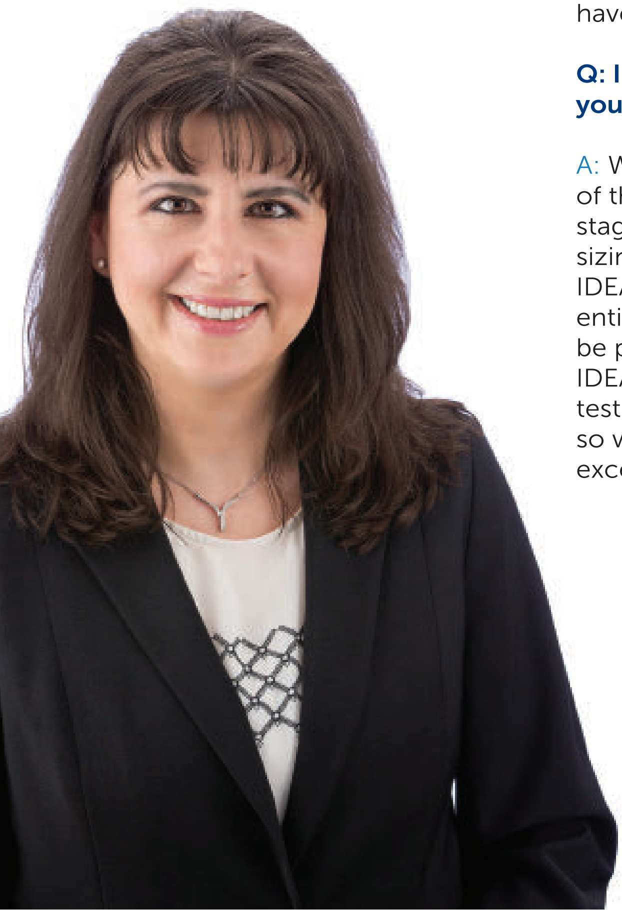
Lessons Learned

- The risks presented by this type of partnership can be mitigated in a variety of ways, including the nonfinancial partner reviewing bank statements and cancelled checks, receiving automated financial reports directly from the accounting system, or having an outside accountant review information periodically.
- Agreements related to formulating business arrangements must provide specifics regarding responsibilities of each party, which auditors can then use as the basis for audit procedures and to establish expectations.
- Internal auditors should work with counsel to ensure compliance with laws and that potential legal impacts of investigations are fully considered.
- In small and medium-size businesses, internal audit should ensure stakeholders participate in the internal control environment. This can include implementing monitoring controls, such as separate individual review of financial reports and involving all necessary parties with external relationships related to financial filings.
- There should always be a secondary review of checks to verify the supporting documentation, payee, and amount are appropriate. Ia

JAMES CARROLL, CRMA, CPA/CFF, CFE, *is manager of Dispute Advisory Services at BDO USA LLP in Pittsburgh.*

AUDITOR SPOTLIGHT

Kronos is a leader in workforce management solutions that enable tens of thousands of organizations in more than 100 countries to control labor costs, minimize compliance risk, and improve workforce productivity. CaseWare Analytics recently interviewed Bistra Dimitrova, MBA, CIA, CRMA and Manager of Internal Audit to discuss why Kronos uses CaseWare IDEA.



Q: Why did your organization start using data analysis software?

A: A few years ago, we had several IT systems housing different operational and financial data that didn't interact with one another. It was challenging to combine the information to create the holistic view we needed to draw meaningful conclusions and produce accurate audit results.

We started looking for a data analysis software that would analyze data from different systems, was easy to implement and use, and robust enough to support our growing business and audit needs. After reviewing several options, we decided to purchase IDEA and we haven't looked back.

Q: In what phase of the audit do you use data analytics?

A: We use data analytics in all phases of the audit. During the planning stage, we use it for scoping and sizing. During fieldwork, we use IDEA because we can analyze the entire population, which would not be possible with manual analysis. IDEA makes it easy to create new tests and narrow the population so we can focus on anomalies and exceptions.

For example, in a scenario where 95% of the population is compliant, we need to identify the 5% that isn't. Data analytics make it possible for us to look for specific infractions or patterns and narrow hundreds of thousands of records to a manageable few.

In reporting, we use data analytics to quantify our results accurately without extrapolation, which makes them much more meaningful.

Q: Which IDEA functions do you love to use?

A: I use all of IDEA's functions! One of the things that I really like is that I can use any file type. It doesn't matter if it is a PDF, .txt or a .csv file, I can throw them into IDEA and extract the information I need.

Recently, I needed to combine two Excel files with 60 tabs and numerous records in each into one file. I was certain that IDEA wouldn't be able to handle the import, but to my pleasant surprise it took the tool less than two minutes to import the files.

All of the data was imported, there were no blank or missing fields, and I could append all of the tabs very quickly. Just a couple of hours later and I was done with my analysis. Imagine trying to append 120 tabs and then manipulating a file of that size in Excel—it would take forever!

To learn how CaseWare IDEA can help you complete your audits more efficiently, visit www.casewareanalytics.com.

CaseWare
ANALYTICS

ON THE R

This year's up-and-coming practitioners are making a difference in their organizations and helping move the profession forward.

The paradigm for young audit professionals is shifting rapidly. Continuing a trend established by each successive group of Emerging Leaders over the last few years, 2017's class started their careers remarkably well-prepared and laser-focused on internal auditing. In fact, some began making career plans as early as high school; and some have returned to their alma mater post-graduation to help educate others on the profession. These practitioners aren't nonaudit professionals who just happened to answer an internal audit want ad. Moreover, they're what might be called "post-IT-literate." In other words, they don't see computer skills as a necessary asset for getting ahead at the office. Proficiency with data and software is assumed; it's been an integral part of their entire lives. They think in terms of maximizing process improvement through data analytics and leveraging sophisticated IT in routine audit engagements. And this year's crop embraces the role of trusted advisor. They're ready to take a seat at the C-suite table, to advise the business on high-level risk assessment and mitigation, and to use their unique perspective to spot problems and opportunities that impact the success of the organization. These ambitious, talented practitioners are steeped in the profession, poised to take on new challenges, and ready to lead.

ISE 2017

Russell A. Jackson

EVERET ZICARELLI

CIA, CPA
27
SENIOR INTERNAL AUDITOR
SALLIE MAE BANK
NEWARK, DEL.

It's time for internal auditors to get the credit they deserve, and **EVERET ZICARELLI** is doing what he can to accomplish that. In fact, the University of Delaware graduate says the profession should place more emphasis on marketing internal auditing as an exciting and rewarding career choice for college graduates. "I'd like to see the profession encourage schools to offer more courses and majors centered around internal auditing," he says "so we can attract talented candidates straight out of college and grow that talent organically." He says he hopes others will have a better awareness of the profession than he did after graduating and working in public accounting. "When I switched to internal audit, I didn't really have a good understanding of the difference between external and internal auditing." Now that he's gotten up to speed on the latter, Zicarelli keeps his external audit skills sharp by leading Sallie Mae Bank's direct assistance program for its external financial statement audit, notes Thomas Linton, the company's vice president, Internal Audit. The team performs audit-related tasks on behalf of the external auditors, reducing the fees and "further demonstrating the competency of the internal audit function." Zicarelli helps enhance that competency through his role with the department's on-campus internship recruiting program—and, Linton points out, he's been rewarded for his efforts by being tapped as the designated mentor for all internal audit interns. He adds that feedback from past and current interns highlights the role Zicarelli has played in ensuring a first-class internship experience. "My favorite part is their passion for learning," Zicarelli says. "They want to learn it all and can't wait to take on the next challenge. That's extremely rewarding."

KAREN TYLINSKI

CFE
29
SENIOR AUDITOR
NIELSEN
TAMPA, FLA.

KAREN TYLINSKI sees things differently—and she tries to help others do so, too. She started at her current company with a background in tax at a Big 4 international accounting firm, notes Kevin Alvero, senior vice president, Internal Audit, at Nielsen. Since coming on board, the University of South Florida graduate has shared audit techniques from the tax field "that have benefited us in the audience measurement industry," he says. Tylinski's efforts include researching new audit tools and helping automate previously manual audit procedures, and she's leading a large internal audit engagement that could have a multimillion-dollar impact on the business. Alvero adds: "This is indicative of the level of comfort I have in her leadership skills." Tylinski says experience helps her build confidence, which makes the job even more rewarding. She says she has a better understanding and awareness of how her work fits into the big picture, for the department and the company, which makes it more fulfilling. She says she hopes to spread the word, showing future practitioners how exciting internal auditing is. "Internal auditing keeps me on my toes, especially since no two projects are the same," she says. "I would like to help people outside the profession understand how stimulating and rewarding it can be."

> **"Internal auditing keeps me on my toes. ... I would like to help people outside the profession understand how stimulating and rewarding it can be."**

KARA GOSLIN

CIA, CPA
29
SENIOR INTERNAL AUDITOR – EMEA
DECKERS OUTDOOR CORP.
LONDON

KARA GOSLIN wants to make internal audit better on the inside—and from the outside. Sarah Eberhardt, chief audit executive at Deckers Outdoor Corp., recalls Goslin's response to feedback about U.S. Sarbanes-Oxley Act of 2002 testing tools that were slow and not user friendly. The University of California at Santa Barbara graduate helped choose and develop a new tool, and was very involved in streamlining the internal testing process. She also successfully presented a business case to Eberhardt and the company's chief financial officer for her current assignment to London, her home base for helping improve Sarbanes-Oxley testing in Europe, the Middle East, and Africa—and for networking globally within the company. She has also created training materials and conducted coaching sessions with local leadership. Moreover, Goslin wants to update internal auditors' demographics, noting it is "a field that becomes much more male dominated the higher in management you rise." She says the paradigm is shifting, but emphasizes that the profession still has a long way to go in terms of women's visibility and progression. Indeed, Goslin sees internal audit departments tapping practitioners with more varied backgrounds moving forward. "A lot of departments have rotational programs," she says. "That's important in broadening our understanding and identifying where we should be focusing." She adds that it could help change how outsiders see internal auditors. And while she's amused by people who picture "a tight-laced numbers person trying to dig up dirt," she stresses the importance of countering that false impression. Goslin looks forward to the day when nobody is surprised that a woman, musician, and craft beer aficionado is also an internal auditor.

BRIAN SALVADOR

CPA
29
SENIOR INTERNAL AUDITOR
INTELLECTUAL VENTURES MANAGEMENT LLC
BELLEVUE, WASH.

BRIAN SALVADOR likes to get things done—and if they don't work correctly, he likes to fix them. He offered dozens of project performance improvement suggestions to his previous employers EY and Boeing, says Colette Pretorius, Salvador's former boss at Boeing and now group finance manager at Microsoft. The Portland State University graduate once led a control assessment at a major sports promotion company with personnel scattered across three continents and led testing of Sarbanes-Oxley controls for two Fortune 500 companies. Notably, he also developed a risk control matrix repository—based on engagement and control types—to improve quality and consistency in workpaper documentation, saving one client more than 4,500 hours. "I noticed that auditors were always drafting audit programs from scratch," Salvador says. The tool was well-received and now serves as a model to new auditors developing work programs. But there are bigger changes he'd also like to effect, moving the profession from "primarily providing process assurance to providing proactive consulting, helping the organization improve internal controls and underlying systems in a manner that positively impacts downstream activity." He notes as well that technology-savvy and mature organizations will shift toward automation, requiring further proactive efforts from practitioners. "It's important for internal auditors to understand the tools available to analyze data—and to educate their businesses on identifying risk areas and evaluating internal controls," he says. Moreover, Salvador anticipates an increase in continuous monitoring, allowing organizations to perform effective trend analyses and better predict changes in their business environments.

DREW WILLIAMS

CIA, CPA, CFE
29
INTERNAL AUDIT SUPERVISOR
RAYTHEON CO.
DALLAS

Adding value to an organization through internal audit engagements is not the same as using those engagements simply to save clients some money. That's a lesson **DREW WILLIAMS** has learned already in less than two years in the profession. "I want to recalibrate how we define *value*," he says. "When I hear the word, my mind automatically goes into thinking I need to find that inefficient process that will save the company millions." In reality, he's discovered, "value" could be as simple as identifying redundant processes, highlighting a manual process that could be automated, or escalating an issue to the appropriate audience. Those are areas the University of Texas at Dallas graduate excels in, notes Sarah Garcia, senior manager, Internal Audit, at Raytheon. "His partnerships throughout the business gain him continued support during audit engagements," she says, "and encourage other audit customers to collaborate with us." He builds and strengthens those relationships in part through regular social outreach, she adds. Williams also effectively wields perhaps the ultimate value-add weapon: data analytics. "I enjoy the challenge of understanding raw data sets and identifying key fields," he says, "then strategically developing criteria to analyze the data to draw meaningful conclusions." Artificial intelligence and robotic software will increasingly assist auditors in managing massive amounts of data, he adds. "Internal audit needs to master these tools. Having facts and data to support a risk assessment—or even to facilitate a conversation—makes life a lot easier throughout the engagement."

JORDAN GROSS

CIA, CPA
29
SENIOR AUDITOR
FOSSIL GROUP INC.
RICHARDSON, TEXAS

> **"I'd like to see internal audit involved much earlier in big strategic projects that affect the business, like a system rollout or a reorganization."**

In the future according to **JORDAN GROSS,** internal auditors will help map out corporate strategy, while computers will track and manage glitches in the system. "The line between a 'financial' and an 'IT' auditor continues to blur," the University of Florida graduate says. He calls on all practitioners to understand the basics of IT systems and governance and how both general and application-level controls work. Auditors of tomorrow will also need to be more adaptable, he says. "The job will evolve away from traditional methods of planning and auditing toward a more continuous audit approach," Gross predicts, "where analytics tools identify and investigate exceptions in close to real time." With just five years of internal audit experience behind him, Gross is already familiar with the big picture. He's Fossil's global Sarbanes-Oxley compliance project manager, says Priscilla Perry, senior internal auditor there, and was recently tasked with bringing a formerly out-of-scope region into the Sarbanes-Oxley testing fold. "[The process] required him to manage the rollout for multiple foreign entities, ensuring controls were mapped appropriately and guidance was provided to new testers and process owners," she says. Perry also notes that Gross is the Fossil data analytics lead, and that he regularly uses innovative thinking to do more with less in an increasingly resource constrained business climate. "I'd like to see internal audit involved much earlier in big strategic projects that affect the business, like a system rollout or a reorganization," Gross adds. "Our ability to emphasize controls when building new processes could greatly reduce the number of issues later."

BILL STAHL focuses on continually enhancing his skill set for an important reason. "In the future, internal auditors must be more broadly versed in the business and be able to leverage technology to detect and monitor risk," the Georgia Southern University graduate says. He notes that operational, business, strategic, compliance, and technology risks will continue to join financial risk on practitioners' radar. Moreover, he says, tomorrow's internal auditors will be required to leverage technology to deliver on-demand results to management. When Stahl uses advanced audit techniques with clients, it often results in the C-suite "changing its approach and seeing the internal audit team as a trusted advisor," notes Steve Jackson, senior manager at EY in Atlanta. Clients often request Stahl by name, a rarity; that may be due in part to his honest approach on engagements. Stahl leads global, multiyear projects with teams scattered around the world, and he relies on his network of internal audit professionals for guidance from time to time. "Internal auditors often are required to audit areas of the business they may not have experience with or be as well-versed in," he points out. "When I have experienced this, I immediately tap my network for the experience or subject matter expertise I need to deliver an accurate and complete audit. From my perspective, having a strong network of leaders and peers you can rely on is critical to being a successful practitioner." He leverages the network of colleagues at The IIA's Atlanta Chapter to expand his areas of expertise, too. The challenge to master more than one competency and to push the limits of the collective internal audit skill set invigorates him more today than when he started in the profession, he says.

BILL STAHL
CIA
28
MANAGER, ADVISORY SERVICES
EY
ATLANTA

ALISSA IRGANG
AMIIA, GDLP
29
SENIOR MANAGER
PROTIVITI
AUSTRALIAN CAPITAL TERRITORY

ALISSA IRGANG thinks big, and acts big. The Australian National University graduate has already served as national lead in Protiviti's first global Project Management Office for a major project, reporting directly to the client executive in New York, notes Jenny Hollingworth, the firm's corporate communications manager. She also notes Irgang's achievement as an author: "Her thought leadership on corporate governance has been published in the *Company and Securities Law Journal.*" Moreover, she's chair of IIA–Australia's ACT Chapter Council, a post she used to create and launch the first IIA mentoring program in Australia, developing the charter and infrastructure and providing guidance for program participants. She's since assisted other states in establishing and managing their own mentoring programs. "The hardest part was the start, because we'd never had anything like it before," Irgang recalls. "Turning this idea in my head into a reality took a lot of time, research, and support." She hopes the mentees learn that the profession is not just about following a defined audit process, stressing that internal auditors need to focus on purpose, not paperwork, and understand the value and objectives behind the audit. She also points out that the technology exists to power a new kind of internal audit practice, working broader, deeper, faster, and smarter. "Everything is changing, and the future is already here," she adds. "To remain relevant, we need to evolve with it."

> **"Everything is changing, and the future is already here. To remain relevant, we need to evolve with it."**

The IIA Atlanta Chapter congratulates Bill Stahl as Internal Auditor magazine's 2017 Emerging Leader

Bill Stahl, CIA

2017 winner of the William J. Mulcahy Excellence Through Leadership Award of the IIA Atlanta Chapter

EY - Advisory Services

Member IIA Atlanta Chapter Young Professionals Group

Inducted into the IIA Atlanta Chapter's C.O. Hollis, Jr. Certifications Honor Roll

13th Annual

The 2018 Atlanta IIA Conference

September 28, 2018

Kennesaw State University recognized as the 4th University in North America and 7th in the world to attain top ranking of Center for Internal Audit Excellence.

KSU Internal Audit Center Advisory Board members pictured left to right Fred Masci, Carley Ferguson, Bill Mulcahy (Chairman) with Center Director Dr. Richard Clune.

The Young Professionals (YP) group within the Atlanta IIA is very active in both the Chapter and the community.

Pictured left to right: Abithia Cunningham (Committee Chair), **Kayla Brown (Emerging Leader 2016)**, Sarah Simmons, Marissa Sorrentino, and **Robin Brown (Emerging Leader 2016)**. Second Row: Ryan Neff, Liz Scanlan Susco, Yousef Ali, Michael Mangrum, **Bill Stahl (Emerging Leader 2017)**, Preston Firmin and Ben Cartoon.

The IIA Atlanta Chapter's mission is to be the premier professional association dedicated to the promotion, advocacy, and development of the practice of internal auditing in the Greater Atlanta Metropolitan Area. This shall include, but is not limited to, the following: Professional development, promotion of IIA certifications, internal audit research and information sharing, and working with universities to promote internal audit education. The IIA Atlanta Chapter worked with Kennesaw State University to establish the first IIA Center for Internal Audit Excellence in the state of Georgia.

The Institute of Internal Auditors · Internal Auditing Education Partnership · IAEP

Certified Internal Auditor

The Institute of Internal Auditors Atlanta Chapter

Kennesaw State University
Coles College of Business
School of Accountancy

15 MAKING A DIFFERENCE

ANNE DAVIS

CIA
26
RISK AND FINANCIAL ADVISORY SENIOR CONSULTANT
DELOITTE & TOUCHE LLP
CHARLOTTE, N.C.

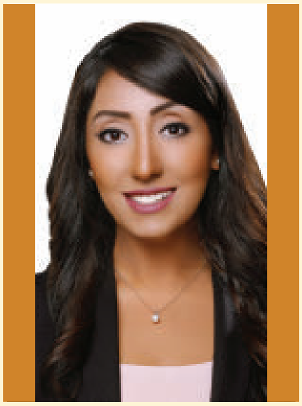
A marketing internship as part of the Wake Forest University Business and Enterprise Management program showed **ANNE DAVIS** that her interests in business were actually more aligned with accounting and finance and, eventually, internal auditing. Now, when she's not traveling for client projects, "she continues to seek opportunities to return to her alma mater, to promote the benefits of a career in the profession," says Paul Lindow, internal audit partner at Deloitte. Davis is also a career coach for Deloitte's summer interns, helping them acclimate to the firm's culture and to the professional services industry. Lindow credits her involvement with enabling a more positive experience for the interns—and with helping them build the foundational skills necessary for a career in internal auditing. The most rewarding aspect? Davis says she truly enjoys sharing her knowledge and perspective about a profession she respects and enjoys, and she's convinced more than a few interns that internal auditing can be challenging, rewarding, and interesting. Indeed, Davis' work focuses on financial services clients, providing her with experience in anti-money laundering efforts and in Dodd-Frank Act supervisory stress testing and Comprehensive Capital Analysis and Review, among other areas. "I'm also learning how to incorporate data analytics, robotics, and cognitive intelligence to execute audits in a more effective way," she notes—streamlining processes and working with the first and second lines of defense to provide a value-driven outcome. That's the kind of approach she says will help "propel the internal audit profession in the right direction and shift the sometimes negative perception of us as troubleshooters into one of trusted, independent partners."

> **"Operational audits combined with technology audits can be a value-add to organizations, but they'll require a complete transformation in the way we work."**

MATTHEW SUHOVSKY

CIA
29
FINANCIAL SERVICES RISK MANAGER
CROWE HORWATH LLP
NEW YORK

For **MATTHEW SUHOVSKY,** relationships are key in internal audit. The California Lutheran University graduate says building them is critical to success in the profession. "This doesn't happen immediately, but as trust is built and success has been achieved," he says. Staying on the same engagements over time helps. "Clients don't only know me as someone who works for Crowe, they know me as a person," he adds. Suhovsky's soft skills extend to co-workers, says Machelle Rinko, senior manager at Crowe. "He recruits and develops talented professionals," she notes, "and builds a successful, dedicated, and motivated team." He also mentors in the organization's formal performance management program, and he seeks a more positive image of the profession. "Internal auditors are here to help mitigate risk and act as a partner and resource to businesses," he stresses, "contrary to the perception of auditors aiming to get people in trouble." He's helping to change that perception through campus recruiting and speaking with students about the profession. He's also looking to the future, and the changes it may bring to internal auditing. "Integrated audits allow business units to get a holistic view of their control environment," he says. "Operational audits combined with technology audits can be a value-add to organizations, but they'll require a complete transformation in the way we work."



NORA ZEID KELANI
CIA
28
GROUP INTERNAL AUDITOR
TRUST HOLDING
AMMAN, JORDAN

NORA ZEID KELANI combines technical audit skills, an ability to see the big picture, and a sharp focus on bringing more women into the profession. "It is a given that in the Middle East, internal audit is a male-dominated career, especially when travel is involved," she says. "Women are discouraged from working in this profession and are often looked at as less professional." She recalls an audit report writing course with 40 attendees—39 men and her. That took courage, says Shafiq Nino, group internal audit manager at Nest Investments (Holdings) Ltd., who also cites Kelani's work with the company's Group Audit Automation project, which entails finding innovative ways of leading teams from a dozen subsidiaries in multiple geographies from a remote location. Nino also lauds Kelani's commitment to education and to women's rights, noting the time the Hashemite University graduate "had a positive influence on a Jordanian woman in her 30s, helping her pursue a college education with support and tutoring." Kelani says it's a matter of effort. "The more the internal audit community puts into changing the inherited mindset of male dominancy, the more women will join us," she emphasizes. The profession needs more young members, too, Kelani says, urging internal auditors to be more proactive by communicating with college and high school students, offering free introductory workshops and Q&A sessions. And while she thinks more and more internal audit functions are adopting forward-looking practices, she notes further progress is needed. "If we want to be a 360-degree business-focused profession and not just a finance-related profession, we need to start being one—now."

The Judges

This year's Emerging Leaders judges see a group of young professionals who want to shake up the status quo, and who possess the background and skills to do so. These qualities should serve them well, as today's practitioners face an audit environment where the status quo is crumbling, and where they're increasingly called to advise on business priorities and emerging risks. To handle that responsibility and effectively partner with management, the judges note, the 2017 Emerging Leaders will have to stay on their toes, keeping informed on regulatory requirements, cybersecurity threats, industry-specific developments, reputational risks, and other key issues. Are they up to the challenge? The judges think so, and they should know. This year's panel represents a variety of geographies, industries, and audit roles – and some are past Emerging Leaders honorees themselves.

KAREN BRADY, CIA, CRMA, *corporate vice president of audit and chief compliance officer, Baptist Health South Florida; member, IIA North American and Global Boards of Directors*

The "age of deregulation" will require tomorrow's leaders to justify their department's value. "This requires not only having the skills to become a valued business partner," Brady says, "but also the finesse to demonstrate this value." That, she adds, is going to make an already challenging profession even more so. But these young professionals have demonstrated strong multitasking skills. "The amount of time they dedicated to volunteerism, as well as their efforts in mentoring, was quite surprising considering the amount of time they dedicate to their full-time job," she says.

KAYLA FLANDERS, CIA, CRMA, *senior audit manager, Pella Corp.; member, IIA Publications Advisory Committee*

Today's Emerging Leaders will not practice yesterday's internal auditing, Flanders explains. "We no longer focus only on compliance and strict enforcement of policies," she says. Flanders is optimistic about the group's experiences in forward-looking areas such as data analytics, audit process improvement, and relationship building. That last skill, she says, is "crucial to the profession's success."

THOMAS LUCCOCK, CIA, CPA, *director, Internal Audit, and senior advisor to the president (retired), Michigan State University; member, IIA Publications Advisory Committee*

More of 2017's Emerging Leaders are called "trusted advisors" by their nominators and peers than in years past, Luccock notes, and that represents the constant evolution of the profession. "The importance of breadth of knowledge and experience, as well as data analytic skills, is becoming paramount to effectively evaluating internal controls," he says. "Today's Emerging Leaders must be aware of the increasing need for cybersecurity controls and how to evaluate these."

15 MAKING A DIFFERENCE

> "The availability and presentation of data is going to change internal audit. Presenting analytical results through visualizations is our next frontier."

JOSHUA WOOD
CIA, CPA, CFE
28
INTERNAL AUDITOR III
CALPINE CORP.
HOUSTON

JOSHUA WOOD is an expert at data analytics. He leads training sessions for his audit department on analytics software and stays current by attending educational events. Rick Hamel, manager, Internal Audit, at Calpine Corp., notes that the Louisiana State University graduate has mastered creating and modifying ACL scripts "to perfect the query to deliver the correct results without numerous false positives." Wood is learning how to transform and interpret data using other analytics software, too. "He understands that data analytics is a powerful tool in any audit," Hamel says, noting that Wood has applied the technology to duplicate payments, payment cards, and payroll data. Wood's contributions also include working with the company's IT groups and business segments to extract data from the applications they use, and use of analytics to evaluate company time sheet compliance with state labor laws. He's also a mentor to multiple interns on the job and is known for "solid planning, work management, and results," Hamel notes. And while he's firmly focused on current practice and technology, Wood also keeps an eye toward the future. "The availability and presentation of data is going to change internal audit," he says. "Presenting analytical results through visualizations is our next frontier."

ANNE MERCER, CIA, CFSA, CFE, *vice president, Internal Audit (retired), Universal American; vice chair, Member Services, IIA North American Board of Directors; member, IIA Global Board*

As a group, this year's Emerging Leaders are well-prepared for the realities of modern internal auditing, Mercer observes. "They're passionate about promoting the internal audit profession," she says, "in part by working within their organizations to educate business owners on the collaborative role of the department." That aligns well, she adds, with the mandate today for practitioners to add value to the organization while also highlighting their unique role compared to other compliance-oriented functions.

MAJA MILOSAVLJEVIC, CIA, *senior group internal auditor, Sberbank Europe AG; 2015 Emerging Leader*

In an internal audit environment that she characterizes as challenging, Milosavljevic says practitioners must "deal with new areas of auditing, such as corporate culture, and constantly develop their skills and knowledge." Accordingly, one of the ways she finds the 2017 Emerging Leaders inspiring is that they see the importance of certification and strive to "distinguish themselves through this dimension of professionalism."

NAOHIRO MOURI, CIA, *chief auditor, AIG Japan; senior vice chair, professional practices, IIA Global Board of Directors*

The way internal audit inspires 2017's Emerging Leaders impresses Mouri, who notes as well the tender age at which many of them have realized it's something of a calling—and the "strong sense of purpose" they show to positively influence others in the profession. They're putting their proverbial money where their mouth is, too, he says, "demonstrating their competence to be trusted advisors in their organizations."

KAREM TOUFIC OBEID, CIA, CCSA, CRMA, *chief audit executive, Tawazun Economic Council; vice chairman, global services, IIA Global Board of Directors*

This year's Emerging Leaders must be agile, Obeid notes, because a fast-changing environment demands that auditors' skills rapidly evolve to align with stakeholders' developing demands; that's how they'll achieve the best results. He has high hopes for these practitioners, calling them qualified, motivated, enthusiastic, and "highly involved in elevating and advocating internal audit."

MARBELIO VILLATORO, CIA, *internal audit integrated project manager, Raytheon Co.; 2015 Emerging Leader*

2017's Emerging Leaders have their work cut out for them, according to Villatoro. "They will be challenged with new risks the profession has never seen," he says, "and their leadership will be critical in ensuring positive change can be created across industries." The good news: These practitioners are well-rounded, and they're genuinely committed to the profession's growth. "They're thought leaders who seek positive change," he adds.

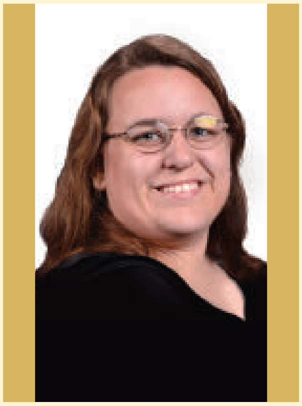
TIANA CLEWIS

CIA, CPA, CFE
29
FOUNDER AND COACH
SELAH FINANCIAL COACHING
MIDLOTHIAN, TEXAS

It doesn't have to say "Internal Auditor" on your business card for you to be an internal auditor. **TIANA CLEWIS** learned that as she recently transitioned from a senior staff auditor position with a large health system to a small business owner focused on financial coaching. Abosede Thompson, senior IT auditor at Baylor Scott & White Health, recalls that Clewis, in addition to volunteering at local IIA chapter meetings, often found innovative methods of addressing project-related challenges. Clewis, for example, took part in an 18-month project to streamline audit access to a third-party web application. The audit showed that too many former employees and contractors retained access to the app. But the audit process was so clunky that it could only be completed every couple of years, creating a significant IT security risk. Clewis was part of the team that undertook the complicated process of changing the app to single sign-on and designing a protocol that can shut down access within 48 hours. "It was a really long process," she says, "but it significantly reduced the number of man-hours needed to audit user access." Now the Howard University graduate—following six years in public accounting—shares her skills with nonpractitioners who need a leg up in their personal financial lives. "I have brought on some wonderful clients who have made great strides in a short time," she reports. She's also started taking on public speaking engagements and just wrote a book called *The Tool Called Money*. "I will always be an internal auditor," she stresses. "It's not a job; it really is part of who you are. If you're always looking for ways to make things more compliant, more secure, and more efficient, you are an internal auditor at heart." And while this mindset remains permanent, Clewis also points to the change and evolution of audit practice itself. Nobody just walks into a client's office anymore with a list of check-the-box questions, she says. "It's about digging into the process and procedures and stepping into the mind of the auditee."

JESSICA MINSHEW

CIA
29
INTERNAL AUDITOR
FINANCE INDUSTRY
MACON, GA.



The faculty at Georgia Southern University focused extensively on external audit when **JESSICA MINSHEW** was a student there. "It was reluctant to even acknowledge the internal audit field," she says. So The IIA's Middle Georgia Chapter, under her leadership as president, recently launched a faculty certification sponsorship program that covers the cost of the Certified Internal Auditor (CIA) exam, and training, for a business or IT faculty member at a local college, turning the newly minted CIAs into campus internal audit advocates. Minshew says her goal is to reach all the colleges and universities in the chapter's footprint. She'd also like to see greater diversity in the profession and bemoans the commonness of overly similar staff backgrounds and stagnant ideas about the role of internal audit. "Bringing people into the department with different backgrounds and specialties, such as psychology or human resources, and strategically using them," she says, "can build relationships with human resources, IT, and other business units that manage sensitive data." Diversity also facilitates designing and performing audits of new and emerging areas—corporate culture, social engineering, or internal communications, for example—that may dominate in the future and help stave off irrelevance. "I believe the only way internal audit will outlive automation is to prove the value of nontraditional audits," Minshew says.

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

ALEX RUSATE

CCSA, CPA
26
SENIOR AUDITOR, FINANCIAL CONTROLS
AMRI
ALBANY, N.Y.

ALEX RUSATE started preparing for a career even before selecting a college, setting his sights on the accounting profession. On campus, an internal audit internship helped steer him toward his current line of work. But he knows that many students don't have that kind of exposure, so he used his time at Bentley University to help teach young people financial literacy. He created a program that taught accounting and finance to high school students—and exposed them to a wide variety of career options. "I thought that was the most rewarding part of the program," he says, "because I could see students with genuine interest in internal auditing and forensic accounting." Anthony Curto, a senior associate at KPMG, who's known Rusate for the better part of a decade, adds that Rusate now helps his alma mater pair students with alumni as academic and professional mentors. On the job, Rusate sees a high-tech future where practitioners "audit smarter by leveraging data analytics and computer-aided audit tools" — and use their detailed understanding of the organization's operations to add value. He'll be ready. Recent accomplishments include conducting an analysis of a former employer's revenue recognition process and control structure and aiding in whistleblower hotline allegation investigations there, too. He also conducted a full regulatory review of a former employer's compliance with the U.S. Telephone Consumer Protection Act.

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

COSO ERM

Getting risk management right

As enterprise risk management (ERM) has become popular in the past two decades, organizations have been trying to implement a program that makes all stakeholders satisfied that they are "doing risk management right." The problem is ERM is not a program. In fact, it is not a department nor a process, either. ERM — or more generically "risk management" — is an integral component of decision-making. It is a set of skills, approaches, competencies, tools, culture, and more that do not stand alone, but are part of all that an organization does. Unfortunately, many organizations don't execute risk management well and suffer the consequences.

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) recently published an update to its 2004 COSO ERM framework. The name of the 2017 version says it all: *Enterprise Risk Management–Integrating With Strategy and Performance*. Risk management is all about strategy and performance.

MAKING BETTER DECISIONS

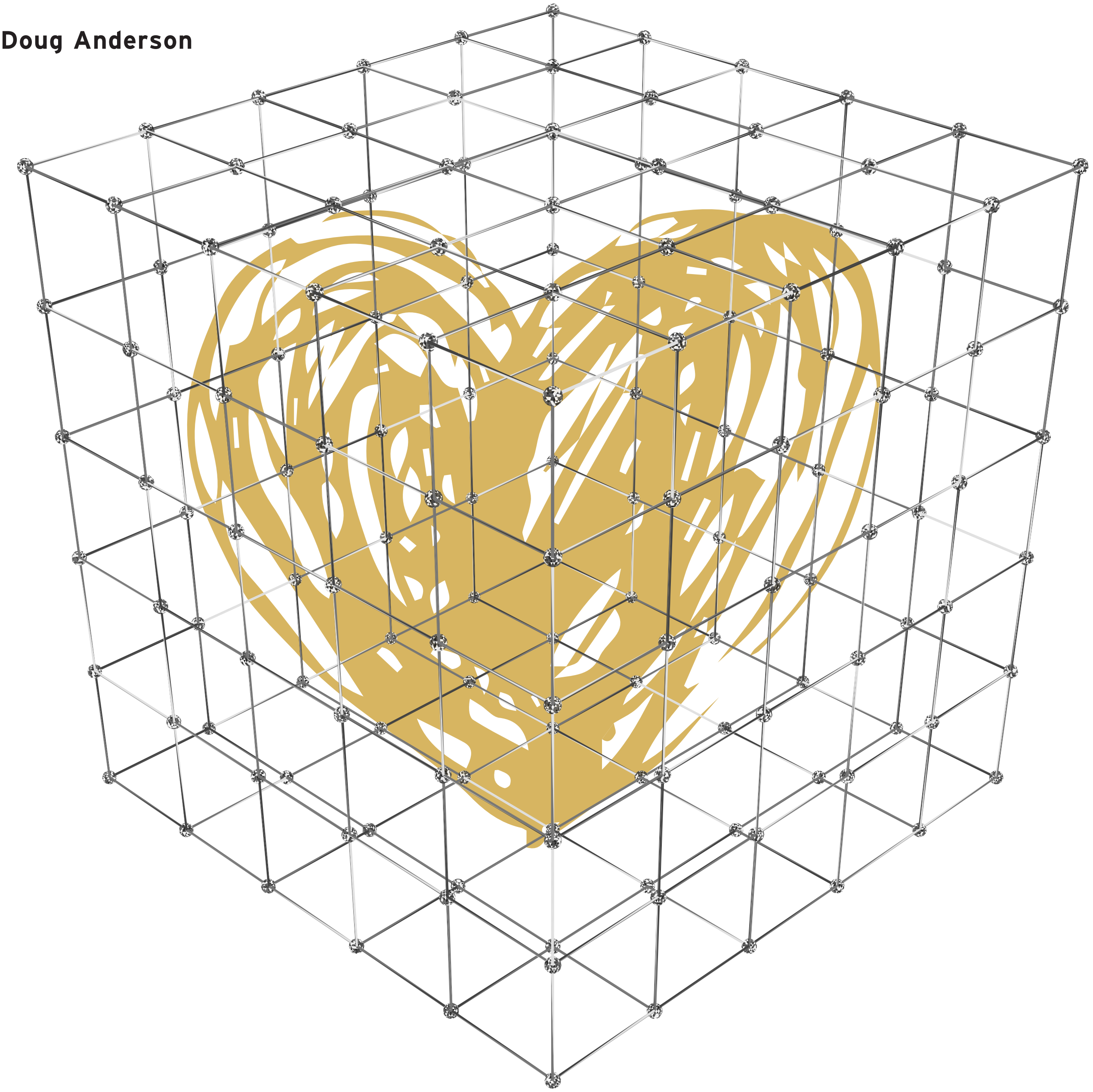
Risk management is an integral part of decision-making. What does this mean? Consider two different situations.

Acme Co. is implementing a new software package to support its core processes such as accounting, logistics, and customer management. As part of its planning, Acme lays out all the steps in the implementation process and then considers what may not go as planned. Some things could go wrong; some could go better than expected. Identifying these possibilities, assessing their importance to the project, taking preparatory actions, and watching how the project progresses are part of how Acme manages its software implementation. This is all done using various monitoring and reporting tools, within the culture of how Acme operates. Acme uses the fundamental aspects of good risk management, even though it may not recognize them as such.

Beta Co. is repainting the exterior of its headquarters buildings. The company turns to its normal painter

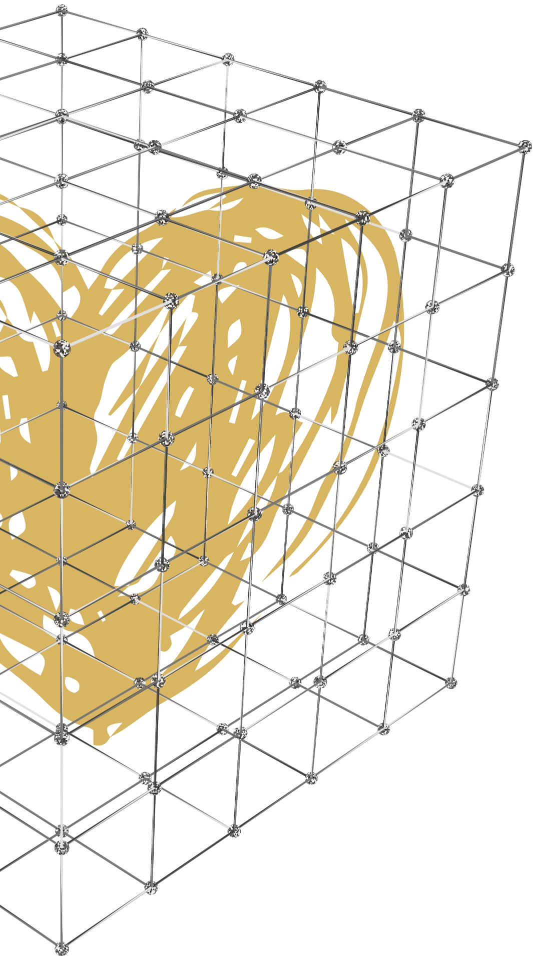
Strategy and organizational performance are the heart of the updated framework.

Doug Anderson



IMAGES: FRAMEWORK, ANTARTSTOCK / SHUTTERSTOCK.COM; HEART, MARISH / SHUTTERSTOCK.COM

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



to get the job done. There also were risks related to this project, but it is less obvious how Beta managed the risks.

Both Acme and Beta made decisions (multiple ones, in fact). Risk management was an integral part of both organizations' decisions. While the risk management may have looked different in the two situations, it was still risk management. Acme took a more formalized approach, outlining its path forward while considering what deviations from this path might occur because of unexpected events (i.e., risks) and planning accordingly. Beta was not nearly as formal, but relied on past habits to try to accomplish its objectives. The questions for both organizations are how good was the risk management and did they use the right approach?

Risk management does not need to look the same for every organization and every decision. It should be fit for purpose, having the level of sophistication, formality, and transparency that is necessary for the importance of the objectives and risks. Both Acme and Beta may have done a great job or a poor job of risk management. It is not the specific activities and formality of the program that matters. What matters is whether management is handling risks the way it should in the situation.

The new COSO ERM lays out a framework for improving risk management so better decisions are made, helping an organization accomplish its objectives. The framework is not another process to be sent to the ERM team or even to a committee of the board. It needs to be incorporated into the fabric of the organization, providing guidance, tools, processes, and many other elements to improve risk management, regardless of the decision being made. The updated framework's executive summary discusses five interrelated components:

- **Governance and Culture.** Governance sets the organization's tone, reinforcing the importance of, and establishing oversight responsibilities for, ERM. Culture pertains to ethical values, desired behaviors, and understanding of risk in the entity.
- **Strategy and Objective Setting.** ERM, strategy, and objective setting work together in the strategic planning process. A risk appetite is established and aligned with strategy. Business objectives put strategy into practice while serving as a basis for identifying, assessing, and responding to risk.
- **Performance.** Risks that may impact the achievement of strategy and business objectives need to be identified and assessed. Risks are prioritized by severity in the context of risk appetite. The organization then selects risk responses and takes a portfolio view of the amount of risk it has assumed. The results of this process are reported to key risk stakeholders.
- **Review and Revision.** By reviewing entity performance, an organization can consider how well the ERM components are functioning over time and in light of substantial changes, and what revisions are needed.
- **Information, Communication, and Reporting.** ERM requires a continual process of obtaining and sharing necessary information, from both internal and external sources, which flows up, down, and across the organization.

CLEARING UP MISCONCEPTIONS

Although the new COSO ERM framework is fairly straightforward, a few

20% of respondents say their organization's risk management process is a strategic tool that provides a competitive advantage, according to the AICPA/ERM Initiative 2017 State of Risk Oversight study.

ISO 31000 UPDATE COMING SOON

The International Organization for Standardization's Technical Committee 262 is updating its ISO 31000 risk management standard. The revision to the 2009 standard is expected to be issued in early 2018. While different in structure, the core aspects of ISO 31000 are consistent with COSO ERM. The standard asserts that risk management is an integral part of decision-making, and creating value for the organization is the primary reason for risk management.

MORE

To download the IIA position paper, The Role of Internal Auditing in Enterprise-wide Risk Management, visit http://bit.ly/2vIU6Mt

key points often are missing in ERM as practiced today.

Risk Is Not the Focus The approach to risk management should not focus on the risks in isolation. The focus should be on those events that can affect the achievement of strategy and business objectives. When the focus is on the risks, and not the strategies and objectives, ERM becomes a program. To add value, ERM always must be about accomplishing strategies and objectives. Management does not think first about risk, but about delivering performance and what can impact that performance.

Risk Is Not an Evil to Be Eliminated Every organization takes risks because the world is not perfectly predictable. Every time an organization takes an action, it takes the risk that its expectations are not correct. Sometimes the events that occur have a positive impact, and sometimes they are negative. Risk is a fundamental part of every organization, but it needs to be managed.

There Are Many Ways to Respond to Risk The framework outlines five basic responses to risk: accept, avoid, pursue, reduce, and share. Internal auditors frequently assume the right response to risk is the fourth option — reduce. This reduction is frequently in the form of implementing internal controls to reduce the likelihood or impact of a risk event. However, this is not the only option and other options may be better.

Risk Management Is More a Skill and Mindset Than a Process When risk management turns into a department, team, or process, it can easily become something separate from management decision-making. Doing risk management right improves decision-making. While many experienced managers intuitively incorporate aspects of good risk management into their normal thinking, almost anyone can benefit from the guidance laid out in the framework. There are clear skills, tools, and mindsets the framework supplies that managers need to learn. Don't relegate them to a few select people who never influence decision-makers.

All of the Framework Is Important What most internal auditors and risk managers would think of as risk management is in the Performance component of the framework, but that would fail to see all five components as critical. All five are interrelated. One can't set risk appetite without an understanding of culture; one can't select risk responses without communicating about risks within the organization; one can't have a great risk assessment approach without the feedback loop to review and improve the process based on learning.

ERM Does Not Compete With Internal Controls The framework eliminates any confusion as to how ERM interacts with internal controls. ERM addresses risks as part of decision-making. In managing some risks, a desire to reduce the risks could be accomplished through internal controls. If this is the direction, then organizations should look to the COSO *Internal Control–Integrated Framework* for guidance on how to implement internal controls effectively.

AN OPPORTUNITY FOR INTERNAL AUDIT

Some internal auditors have responsibility for their organization's ERM approach, some provide facilitation, and some perform assessments of management's design and execution of ERM. The IIA Position Paper, The Role of Internal Auditing in Enterprise-wide Risk Management, provides useful guidance on the options, and limitations, for internal audit's involvement with ERM.

Internal auditors who have a more engaged role in ERM through facilitation, training, etc., will work through the new COSO ERM framework in a fair amount of detail. However, there is a wealth of information in the framework for every internal auditor.

Indeed, the framework is a fabulous opportunity for internal auditors who are not intimately involved in ERM. The increased attention to risk

WE DON´T JUST FOLLOW RULES.
WE HAVE STANDARDS

33% of U.S. companies surveyed align their risk management and strategic planning functions, and 20% have risk-related performance incentives, according to PwC's Risk in Review 2016 study.

management that will come about through the release of the updated framework—and the expected release of an updated version of the International Organization for Standardization's ISO 31000: Risk Management Principles and Guidelines—provides internal auditors with the ability to reorient their work, messaging, and reporting around the way management thinks (See "ISO 31000 Update Coming Soon" on page 41). As internal audit strives to create and protect value for organizations, understanding the principles of risk management better and incorporating them into the practice of internal auditing can pay large dividends. Here are some suggested next steps for every internal auditor.

First, internal auditors should become conversant with the fundamentals of the framework. At its core, internal auditing is all about risk. While most internal auditors focus on the adequacy of internal controls, internal controls should be viewed as a method to implement the "reduce" response to risk. Risk is central and comes first, however. Internal auditors should master the concepts of risk—how it is identified, assessed, analyzed, responded to, reviewed, and reported. Without this context, it is not possible to effectively address internal controls.

Second, auditors can do themselves a favor if they talk less about the adequacy of internal controls and talk more about risk, managing risk, and reducing risk where advised. Management thinks of the world through the perspective of setting out objectives and accomplishing them—all with the goal of delivering performance. The more internal auditors talk about those objectives and the events that can impact delivering performance, the more management would understand how internal audit delivers value. Auditors are not here to be naysayers or add bureaucracy with more controls. They are here to help management deliver on its objectives. This requires auditors to think and talk in terms of risk, potential impact, and response.

Third, internal auditors should not only evaluate internal controls, but also management's choice and implementation of risk responses. Internal controls are but one potential risk response. Internal auditors should be considering all five risk responses in assessing whether management has selected the optimal way to address a risk.

Risk responses should be designed to improve performance.

Fourth, internal auditors should not focus blindly on always trying to reduce risk. Risk responses should be designed to improve performance. This involves not only ideas to reduce the impact from negative risk events, but also the cost of risk responses and the possibility of a risk that positively impacts performance. When internal auditors' orientation is toward decision-making and how risks impact performance, they may conclude more risk is appropriate or the cost of current risk responses is not justified by the benefits.

Internal auditors are some of the best in understanding the theory regarding risk. The revised COSO ERM framework provides auditors the opportunity to become even more expert in the material so they can help their organization navigate how best to implement it. Not everyone will see the framework as something worth their attention, providing an opportunity for internal auditors. Ia

DOUG ANDERSON *is managing director, CAE Solutions, at The IIA in Lake Mary, Fla.*

MORE

VISIT The IIA COSO Resource Exchange page at http://bit.ly/2x8smkP to obtain the updated COSO ERM framework and access other risk management resources.

Ia
INTERNAL AUDITOR
APRIL 2017
INTERNALAUDITOR.ORG
Maturity Models: A Tool for Internal Audit
From Intern to Full-time Employee
Stick to the Strategy
Coordinating the Three Lines of Defense
RESILIENCE THROUGH CRISIS
As a key steward of organizational well-being, internal audit can play an active role in making resiliency a part of all operations.

Materiality *Defined*

Michael P. Fabrizius
Sridhar Ramamoorti

Differing concepts of materiality can cause confusion among stakeholders.

Because the term *materiality* arose within the context of financial reporting and statement assurance, internal auditors have been challenged in adapting or creating a definition that is relevant for themselves and their stakeholders. In the context of financial reporting, materiality is relevant to three stakeholder groups: 1) preparers of financial statements, 2) auditors, and 3) users of financial statements. Although materiality decisions are made by only two of these three groups—preparers and auditors—most internal auditors' conception of materiality likely has a user orientation. The auditor might ask, "How would a reasonably prudent investor react to the magnitude of misstatement (under- or over-reported amounts) or omission of a specific financial statement item in terms of its presentation and disclosure?"

Given this backdrop, the term *materiality* can be a significant cause of confusion in determining what to audit, how much to audit, what to correspondingly report, and for what matters it is necessary to gain consensus regarding management action. In many situations, stakeholders come to the table with their own concept of materiality—sometimes vaguely defined—that can be at odds with internal audit's definition. Sometimes managers attempt to mitigate or downplay an issue and internal audit's proposed recommendation because it reflects poorly on their performance in their respective areas of responsibility. In such instances, supposed lack of materiality can be used as the basis for an argument to convince internal audit that the issue under discussion has no real merit.

If internal auditors are not well-prepared to articulate and defend what they believe to be the relevant concept of materiality, the discussion of audit issues can easily become contentious or seriously impaired. It is therefore imperative that internal auditors fully understand the meaning and contexts of the term *materiality* so they are prepared to use it authoritatively and appropriately.

THE OLD RULE OF THUMB

Historically, many stakeholders, and even many internal auditors who began their careers as certified public accountants or chartered accountants, were introduced to the materiality concept from a financial reporting and external audit standpoint. Here, the term referred to the significance of an item to the users of a set of financial statements, and the probability that its omission or misstatement would influence or change a decision by them. Although professional standards never defined the threshold for materiality as a fixed percentage of revenue, equity, or other financial statement value, and it is clear that qualitative factors play an equally important role as quantitative considerations, a widely used rule of thumb was that materiality was reached when a misstatement or omission was at least 5 percent of a given factor—such as net income or net assets. Accordingly, anything less than 5 percent often was considered immaterial for audit scoping or adjustment proposal purposes.

In 1999, the U.S. Securities and Exchange Commission's (SEC's) Staff Accounting Bulletin 99 (SAB 99) rejected the blanket concept that a misstatement or omission of less that 5 percent of a given factor is immaterial. The SEC had no objection to the rule of thumb as a starting point in assessing materiality, but quantifying in percentage terms the magnitude of a financial reporting misstatement was only the beginning of an analysis of materiality.

SAB 99 requires that a determination of materiality for financial reporting consider the quantitative and qualitative aspects of the matter under analysis as part of a full examination of all relevant considerations. Qualitative factors to consider in the materiality evaluation for financial reporting may include reaching budget or other projections, triggering or increasing executive compensation, masking a change in financial results or other trends, and achieving compliance with debt and other covenants. Combining quantitative and qualitative factors can make the materiality determination much more complex. The result of the SEC's pronouncement was to make the old rule of thumb outdated even for financial reporting.

Before the U.S. Sarbanes-Oxley Act of 2002, materiality also was used in identifying serious weakness in internal control over the financial reporting process. The American Institute of Certified Public Accountants defined material weakness as a condition where the internal control components do not reduce to a relatively low level the risk that:

- Misstatements caused by errors or fraud in amounts that could be material in relation to the financial statements may occur.
- Misstatements are not detected timely by employees in the normal course of performing their assigned functions.

In an attempt to establish more consistent and clearer guidance for Section 404 of Sarbanes-Oxley, the U.S. Public Company Accounting Oversight Board (PCAOB) defined a material weakness differently, and effectively developed three categories of financial reporting controls weaknesses (see "Categories of Financial Reporting Controls Weakness" on this page). Under PCAOB Auditing Standard (AS) 5 (now codified as AS 2201), "The severity of a deficiency depends on:

- Whether there is a reasonable possibility that the company's controls will fail to prevent or

CATEGORIES OF FINANCIAL REPORTING CONTROLS WEAKNESS

Three categories differentiate the severity of weaknesses based on level of impact on both the financial statements and the underlying processes that provide data and information.

Category	Definition of Control Weakness
Insignificant Deficiency	A deficiency in internal controls that would not adversely affect the organization's financial reporting process and the critical processes that provide data and information.
Significant Deficiency	A deficiency in internal controls that could adversely affect the company's financial reporting process and the critical processes that provide data and information.
Material Weakness	A significant deficiency or aggregation of significant deficiencies in internal controls that could have a material effect on the financial statements.

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

INTERNAL AUDIT COMPARED TO EXTERNAL AUDIT

	Internal Audit	External Audit
Scope of Work	Controls for operations, safeguarding assets, compliance, and reporting reliability	Financial statements and related controls and processes
Review and Testing Level	Lower	Higher
Range of Risks	Broad	Narrow
Time Horizon	Current, with identified issues projected to future consequences	Historical data
Issue Description	Both nonquantifiable and quantifiable	Quantifiable
Materiality Focus	Efficiency, effectiveness, competitive, customer service, regulatory, public perception, continuity, etc.	Financial reporting

detect a misstatement of an account balance or disclosure.

» The magnitude of the potential misstatement resulting from the deficiency or deficiencies."

Consistent with the SEC's approach, the PCAOB in its standards avoids suggesting quantitative guidelines. The PCAOB says that materiality should not be based on a numerical formula because the facts and circumstances need to be professionally evaluated and considered for each situation.

Not surprisingly, when performing their Sarbanes-Oxley Section 404 assessments, many organizations find it difficult to differentiate between significant control deficiencies and material weaknesses. The organizations and their external auditors often still resort to quantifiable measures of specific impact to the financial statement to help establish a distinction.

INTERNAL AUDITING AND MATERIALITY

Unfortunately, quantifiable rules for materiality continue to be applied even to situations other than the fairness of the financial statements. However, for internal auditors the argument against using any materiality rule of thumb is amplified by the inherent and substantial differences between the roles of internal auditors and external auditors. In summary, very different assurances are provided by these different services. Internal auditors review and test controls at a significantly lower level of materiality than do external auditors, and routinely review a much broader range of risks than those for financial reporting. External audits are designed to report on historical data, whereas internal audits are generally focused on the efficiency, effectiveness, and compliance of current and future operations (see "Internal Audit Compared to External Audit" on this page).

DEALING WITH THE ISSUE

Internal auditors need means of measuring, assessing, or judging the performance of a broad swath of matters that are subject to audit. In the most general sense, the standards used for this purpose are referred to as audit criteria. Audit criteria are reasonable and attainable standards of performance and control against which compliance, the adequacy of systems and practices, and the efficiency and cost-effectiveness of staffing activities can be evaluated and assessed. To be realistic and useful, these criteria must be relevant, reliable, neutral, understandable, and complete. The aggregate of the internal auditor's findings measured against the criteria, along with the exercise of professional judgment, permits the audit team to form a justifiable and defensible conclusion about each audit objective. An important threshold factor is the concept of materiality.

At times, internal auditors may be inclined to avoid dealing with complex concepts of materiality and significance. They may be tempted to throw up their hands and let someone else—senior management or the audit committee—make the call on the importance of identified issues and the need for corrective action. In this scenario, all issues would be delivered in an unfiltered and unprioritized fashion, with internal audit merely performing the role of information gatherer and reporter. Many reasons exist as to why this approach would represent a sort of professional malpractice, and would likely lead to dissatisfaction with internal audit's performance by its key stakeholders.

Different individuals evaluating similar facts may reach different conclusions.

While internal auditors may frequently be confronted with issues that defy simple categorization and prioritization, they need to recognize their responsibility to provide an assessment of significance. Internal auditors are the experts on internal controls and that, by necessity, includes determining the impact that the quality of controls has on their organization's activities.

The *International Standards for the Professional Practice of Internal Auditing* require internal auditors to add value and help improve the organization's operations. They shortchange the value proposition if they do not demonstrate how their work product can directly meet these requirements. By sorting through the information they have gathered in their internal audit assignments, which necessitates the explication of internal auditors' materiality judgments, they can move forward with the important and leave behind the unimportant.

Granted, this is not always an easy task. There is no mechanical application of a framework that will provide simple, indisputable answers. Because of the need to apply professional judgment and to consider and weigh many factors, different individuals evaluating similar facts and circumstances may reach different conclusions in certain situations. When this happens, internal auditors have to deal with the gray areas of the issue.

The *Standards* allow internal auditors to permit senior management to accept a level of residual risk, if they do not believe it is unacceptable to the organization. However, as stated in Standard 2600: Communicating the Acceptance of Risks, if internal auditors believe it is "unacceptable to the organization, the chief audit executive must discuss the matter with senior management. If the chief audit executive determines that the matter has not been resolved, the chief audit executive must communicate the matter to the board."

Any other difficult issues may also require further attention to move them to consensus. This could involve the engagement of specialists, internally or externally, who provide subject matter expertise. Also, these very limited, infrequent, and contentious issues could be just the ones that are significant enough that involvement by senior management or the audit committee may be needed to reach resolution.

Issues that advance to this level should meet criteria that are established

Companies that focus on **material issues** report up to 50% **added profit** from sustainability activities, according to MIT's Corporate Sustainability at a Crossroads report.

and understood in advance by internal audit, senior management, and the audit committee with an agreed-upon reporting protocol. Stakeholders typically express interest in categories of topics and issues, such as fraud and significant regulatory noncompliance, about which they want to be made aware and involved, regardless of materiality. To cover the other possibilities that require some assessment of importance, it is necessary to have a working definition of materiality for internal auditors and their stakeholders.

GUIDELINES FOR MATERIALITY

When evaluating the significance of the issues that audit work identifies, some guidelines can supplement the definition (see "Definition of Materiality for Internal Auditing" on this page), help frame the evaluation, and determine significance. These guidelines help with the application of materiality in practice.

DEFINITION OF MATERIALITY FOR INTERNAL AUDITING

MATERIALITY for internal auditing was defined in a 1994 IIA research report, The Internal Auditor's Role in Management Reporting on Internal Control, as "any condition that has caused, or is likely to cause, errors, omissions, fraud, or other adversities of such magnitude as to force senior managers to undertake immediate corrective actions to mitigate the associated business risk and possible consequent damages to the organization."

This definition is particularly relevant because of its general management perspective, not just a financial perspective. It also is risk based, enterprisewide, and action-oriented in dealing with risks.

While the revised and updated International Professional Practices Framework does not define the term *materiality*, the Glossary does contain the following definition for the term *significance*: "The relative importance of a matter within the context in which it is being considered, including quantitative and qualitative factors, such as magnitude, nature, effect, relevance, and impact. Professional judgment assists internal auditors when evaluating the significance of matters within the context of the relevant objectives."

Materiality for External Auditors May Not Be Relevant Do not base materiality for matters of operational efficiency and effectiveness, safeguarding assets, and compliance with laws and regulations on the materiality concepts and levels considered by the external auditors for purposes of the examination of the financial statements or the Sarbanes-Oxley Section 404 internal control assessment. Very different assurance is being provided.

Incorporate Contextual Considerations Materiality should never be used as a sole or significant measure for prioritization and investigation in cases of suspected or illegal behavior or fraud. Put another way, zero tolerance or allowable error of zero should be established when considering illegal acts.

Consider Qualitative Factors The qualitative dimensions of an issue may be more important than the quantitative aspects. Customer service, public perception, cycle time, quality outcomes, and employee morale are examples of important considerations that are resistant to quantification efforts.

Context Matters Remember that not all quantifiable areas are the same. For example, the significance of errors and misstatements will be different for suspense accounts and related-party transactions because they involve greater risk than most other accounts or activities with similar balances.

Is It Pervasive or Isolated? Understand the root cause of the issue. The fact that it has or can easily recur makes it more of a concern than an isolated, explainable, one-time matter.

Improve Performance Lost opportunities to quantifiably enhance revenues and reduce and avoid costs, while not technically material or relevant to the current financial statements, can be materially important, and have a cumulative effect, in improving performance in future periods.

BUILD A FOUNDATION

A foundation of dialogue with stakeholders can help internal auditors determine a mutually agreed upon framework based on quantitative and qualitative factors. Providing meaningful context to their reporting of issues can enhance internal auditors' value to their organizations and assist stakeholders in establishing priorities, determining remediation, and escalating issues when necessary.

MICHAEL P. FABRIZIUS, CIA, CPA, *is editor-in-chief of the professional journals for the Association of Healthcare Internal Auditors in Charlotte, N.C.*

SRIDHAR RAMAMOORTI, PHD, CIA, CPA, CRMA, *is an associate professor of accounting at the University of Dayton in Ohio.*

Digging *for*

knowledge

Business acumen within internal audit teams reinforces their value and reduces their limitations.

Arthur Piper

Illustration by Sean Yates

Every month, Jorge Badillo, internal audit manager at SCM Minera Lumina Copper Chile, leaves company headquarters in Santiago and takes a two-hour flight followed by a three-hour drive to the organization's mines in the Atacama Desert. Donning a hard hat, he inspects the mines and makes sure he understands the issues that arise in the pit and plant. "The mine site is where things in this business happen," Badillo says. "Internal audit's job is to fully understand the everyday challenges the company faces."

Next year, for the first time, Badillo and his three-person audit team will carry out what he calls a water balance audit. Water is a key resource in the extraction industry, but a scarce resource in the desert, and the company must comply with statutory rules and regulations. The audit will look at how much water comes into the mine, how much goes out, and the level of recycling the mining process entails. This will provide third line of defense assurance to the continuous checks already carried out by management. His audit will aim to identify opportunities to improve how water is used and controlled. Badillo will use a subject matter expert from his cosourced audit supplier to help, with the understanding that there will be knowledge sharing between the service provider and his team.

"We'll get a deeper understanding of the audit process, a more rigorous audit, and, in future engagements, we'll be able to do more of it ourselves," he says. "Building such business knowledge is critical to audit's ability to serve the organization." Badillo's team conducts audits on explosives used to mine raw materials, but, he says, without in-depth knowledge of the type and nature of the explosives used, the team would merely be doing a purchase-to-pay audit. Management needs an assessment of the quality and effectiveness of the explosives, themselves, which takes the audit to another level in terms of its value to the company.

Badillo applies a risk-based audit approach in developing the rolling five-year internal audit plan. About half of all audit engagements have an operational focus, such as fuel management, reagents management, logistics and shipments, and other core business areas. For that reason, business acumen is a prerequisite for success.

Building business acumen within the audit team has never been so important. With fast-changing geopolitical events; disruptive business models; and the increased impact of digitalization on business products, processes, and services, internal auditors need to know their organizations inside out if they are to provide effective and relevant audits. Aligning with the business strategy and objectives, creating a culture of learning within the audit team, and rotating experts through the audit department can all help.

"Building such business knowledge is critical to audit's ability to serve the organization."

Jorge Badillo

REDUCING LIMITATIONS

Before Badillo relocated to Chile from Ecuador and joined the mining industry, he worked in banking, oil and gas, and in a Big Four firm, but knew little about his new sector. Since then, he has put himself and his team through an intensive, continuous self-learning process to develop the business acumen needed to do their jobs well. That has included subscribing to industry newsletters, understanding movements in the copper markets and the cycles of the industry, meeting regularly with management, and going to mine sites where most of the 3,000 employees and contractors work. At one point, he enrolled in engineering classes. "I was the only accountant in the course—the rest were engineers who wondered what I was doing there," he says. Badillo also has had to learn about the Japanese parent company's audit culture and approach. And he cofounded the Internal Audit Group within the Mining Council—the sector's industry body in Chile.

"Auditors need to recognize they have limitations," he says. "So, the first step is to make the decision to acquire the knowledge you need to reduce those limitations. You can never know everything, but the more you show an interest in the business and seek to understand it, the more support and credibility the audit team will build."

Business acumen has been a buzzword in internal audit for several years, but what does it mean in practice? "When we are talking about business acumen today," Larry Harrington, vice president, Internal Audit at Raytheon Co. in Waltham, Mass., says, "we are talking about things like being able to help organizations deal with speed of change by having sound judgment, a quick mind, a sense of the business's vision and strategy, and having the ability to select the right course of action in uncertain times."

"You cannot have a plan that is full, but that contains assignments of limited impact."

Derek Foster

IN TUNE WITH THE BUSINESS

With the amount of rapid change in the business world, Harrington says being able to build an audit team with business acumen is critical to its success. "Every major company is having

Business impact is the **No. 1** measure desired by CEOs, followed by return on investment, when it comes to learning & development, says LinkedIn's 2017 Workplace Learning Report.

to transform itself and needs an internal audit team with business acumen to help it lower costs, improve efficiencies, and see ahead so it doesn't become the next obsolete business."

Raytheon has been developing a culture of learning around the three main knowledge areas that Harrington says auditors need to be on top of. First, they need to have a firm grasp of their organization's strategy and goals. Second, they need to understand the trends facing the industries in which they operate. Finally, they need to get up to speed with how technology is transforming everything from homes to production lines and global communications to personal relationships.

"Those tools will help the audit team build relationships, interdependencies, and networking opportunities within the business," he says. "We need to help with the transformation of our businesses and drive positive change—and for that we need to have deep understanding and connections throughout our organizations."

Raytheon is fortunate to have a large audit shop of 40 people. About one-third of its auditors come from traditional finance and accounting backgrounds—the rest are hired from the business and, over time, have come from every function in the company. It also has a wide-ranging audit charter that provides the remit to go well beyond compliance work.

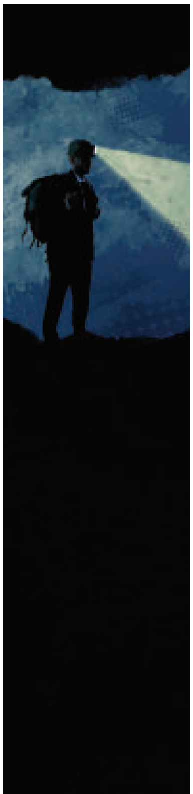
"It is true that not all internal audit shops have a broad charter and some have to focus on financial controls or regulatory compliance," Tom Sanglier, audit director at Raytheon, says. "But that should not prevent those auditors from having meaningful and insightful discussions with stakeholders about the business and its objectives."

LACK OF FOCUS

In fact, large teams sometimes fail to develop sound business acumen, often because they fail to grasp just what it is that internal audit can offer the business. Derek Foster, former CAE at the U.K. postal service Royal Mail in London, says how internal audit sees its role within the business can have a major impact on its ability to deliver insightful, business-oriented recommendations and advice.

For example, internal audit can be understood as a professional support service within an organization in the same way that legal, procurement, finance, and other departments are. "That can be a trap in itself," he says. "It can lead the function to focus too much on its technical and professional proficiencies, rather than also taking a route that will lead to providing more of a commercial perspective on risk in light of the business' strategy and objectives." Some audit functions have failed to shake off their historic focus on compliance, where business acumen is less valued in audit findings than tick-box exercises revolving around the adherence, or otherwise, to established policies and practices, Foster adds.

Some functions have failed to shake off their historic focus on compliance.



Either way, these shortcomings in taking the needs of the business seriously can reduce the quality of audit work. Foster says the audit plan at Royal Mail was linked to the business's objectives to ensure that often scarce internal audit resources were deployed most efficiently. "You cannot have a plan that is full, but that contains assignments of limited impact," he says. "When we did our risk-based plans, we asked, 'why should this audit make the cut?' The decision to include

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

it was based on the importance of the audit to the business's key objectives."

That lack of focus from limited business knowledge and understanding can equally feed into the scope of individual audit assignments. Within any audit project, auditors need to be constantly reviewing and spending time on high-impact areas. "Insufficient acumen will lead to time spent on processes that do not matter to management or the business," Foster says. Finally, one of the hallmarks of an underperforming internal audit function is that its recommendations are not proportionate or commercially sound. "Again, a result of insufficient acumen," he adds.

ONGOING EDUCATION

When the shortcomings of having too little focus on business acumen are written in black and white, they seem self-evident. So, why do too many chief audit executives (CAEs) fail to develop their teams' understanding of the business to a high enough level?

"Throughout my whole career, internal auditors have been criticized for not understanding the business well enough," Bob Rudloff, senior vice president, Internal Audit, at MGM Resorts International in Las Vegas, says. "It's certainly true that some CAEs do not structure their teams well enough, so there can be too many junior auditors on an assignment who don't have even a simple level of business knowledge."

That can easily happen when CAEs get so caught up in delivering their audits that they fail to maintain an effective development program for their auditors. Rudloff says such programs are crucial for helping auditors improve their understanding of the business and need to go well beyond any onboarding initiatives that aim to give auditors an initial orientation of the department and its role in the business.

At MGM, Rudloff has created a program of events, such as bringing in speakers from different parts of the business to share knowledge and answer questions. He encourages staff members to attend local IIA chapter meetings and often arranges panel discussions within the business that can be attended by anyone from the head of legal to the chief financial officer or chairman of the board. Past learning exercises have required individual staff members to read the latest business thought leadership books, summarize the contents, and share them with the team.

That program goes hand in hand with more formal training. "At MGM, we have had a big push for internal auditors to become certified and go through the CIA learning process," he says. "We make the tools available for classroom and self-study, exam preparation, and so on. A CAE cannot be shortsighted and fail to provide that ongoing education."

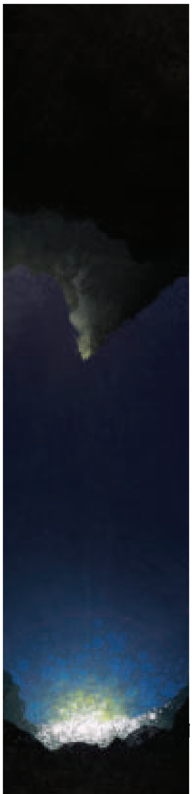
"A CAE cannot be shortsighted and fail to provide that ongoing education."

Bob Rudloff

Younger auditors require more coaching and encouragement than in the past.

While he sees such dual-track programs as essential prerequisites to developing auditors who are both technically proficient and business savvy, he says younger auditors require more coaching and encouragement than in the past. That can put more of the onus for bringing them up to speed with the business onto the CAE and the senior audit team. In addition, the team at MGM Resorts has grown from 25 to 75 auditors in Las Vegas and another 25 located throughout the U.S.

"The business dynamic may be different in Michigan than in Las Vegas, and that needs to be reflected in how auditors at those sites understand the business and what it is trying to achieve," Rudloff says. "As a leader, you



57% of chief audit executives are not convinced their teams have the expertise to deliver on stakeholders' expectations, according to Deloitte's 2016 Global Chief Audit Executive survey.

have to be committed to doing this in the limited time you have, despite these difficulties, because if you don't do it, you will be selling yourself and the business short."

ROTATING EXPERTISE

Building business acumen is not easy even in a small team, especially in an organization whose activities have little to do with finance or accounting—traditional internal audit educational backgrounds. Using cosourced internal audit services and recruiting from outside the audit function (secondments) to share knowledge on such issues as cyber risk and IT are two ways to build acumen.

"We have always had engineer secondments in our audit shop, and it has always been successful," Jade Lee, director of Internal Audit at AltaLink Management in Calgary, Alberta, says. "Those engineers come out at the end of the secondment and invariably move into a more senior position within the energy infrastructure company." Some move out of audit and become managers within the business. Junior engineers tend to secure more senior engineering positions after serving in audit.

In AltaLink's audit function of six people, one is a secondment from the business. Currently, there are another two internal hires from other departments. Those people come into auditing with no technical audit skills, but they bring business knowledge at a level of granularity that is difficult for auditors to acquire.

"We can teach them the audit process, but they have to come with the right mindset and personality," Lee says. "They need to be inherently curious, be able to ask good questions, and they often have a good sense of what is risky in the business because of their hands-on experience."

She says it also can add credibility because the auditors can speak to engineers in the business on a more equal level in terms of knowledge and understanding. "It gets us away from people feeling that the auditors don't understand the technical side of what they do but are asking them to change it. It's more of a conversation," Lee says.

Learning what's important to the business takes time and effort.

"We can teach them the audit process, but they have to come with the right mindset and personality."

Jade Lee

Secondments are supposed to last 12 to 24 months, but Lee has had someone stay for four years. The benefit is that they are working on cross-functional projects across the business and often are speaking to executives with whom contact would be rare if they were still on the shop floor. At the end of their time in audit, they do an open-door lunch-and-learn where anyone can hear what audit is about and what to expect from such a placement. The events act as a showcase for others in the business who may be interested in joining the audit team for a while.

MAKING IT HAPPEN

Audit teams with strong business acumen deliver more detailed, nuanced, and transformative audits for their organizations. But learning what's important to the business takes time and effort, and it has to become part of the audit team's culture—not an add-on project that will inevitably fizzle out. "People without business acumen become extinct in today's environment on a regular basis," Raytheon's Harrington says. "Those who don't go extinct refuse to accept the status quo on their supposed limitations and make positive change happen." Ia

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

assessing soft controls

Control self-assessment can be a powerful tool to address repeat audit findings.

Israel Sadu

An increase in repeat findings often is an indication that the root cause of a control weakness has not been addressed adequately. Frequently when auditors provide similar recommendations, the root causes of these control weaknesses can be traced to human factors. Consider the five P's of effective controls for organizational success: One may design a well-conceived *policy*, a well-designed *program* aligned with the policy, effective *procedures* to implement the program, and well-suited *practices* for following the policy. However, if the organization's *people* do not follow those practices, it defeats the work of implementing the policy.

While management is responsible for setting good internal controls, implementing them depends on people at all levels of the organization. Therefore, it's the soft controls that make a difference. These soft controls are intangible controls such as morale, integrity, ethical climate, empowerment, competencies, openness, and shared values. They differ from hard controls such as organizational structure, delegation

IMAGES: COMPASS, BOHBEH / SHUTTERSTOCK.COM; MAP, POCKYGALLERY / SHUTTERSTOCK.COM

of responsibility, and human resources policies. However, soft controls can significantly impact the effectiveness of the organization's internal control structure.

Despite this impact, internal auditors typically focus on reviewing hard controls because it is difficult to obtain evidence of noncompliance with soft controls. This may be because of insufficient experience or skills in testing the soft controls. However, internal audit has a significant role to play in helping management evaluate soft controls. When seeking to identify risks stemming from soft control weaknesses, auditors can use control self-assessments (CSA) to facilitate the identification and evaluation of risks without impairing internal audit's objectivity. The robustness of CSA processes not only provides a powerful means of addressing these risks, but may also help reduce the likelihood of repeat audit findings that can be a drain on internal audit resources.

> The CSA approach can transfer knowledge among the owners and implementers of the processes.

FACILITATING THE CSA

CSA is a process through which internal control effectiveness is examined and assessed through workshops, surveys, and management analysis facilitated and assisted by a subject-matter specialist. Participants, who are typically management or work teams directly involved in a business function, identify the risk factors, assess the control processes, develop action plans to reduce risks to acceptable levels, and determine the likelihood of the entity achieving the intended business objectives. Internal auditors usually are involved in the CSA process as facilitators because of their expertise and experience with both the organization's business and its related risks and controls. Indeed, The IIA has offered a specialty Certification in Control Self-Assessment since 1999.

CSA differs from the traditional internal audit approach to assessing control effectiveness. Traditionally, auditors were responsible for evaluating and reporting on the risks and effectiveness of controls. With CSA, these tasks are performed by the business units, work teams, or resident experts, and internal audit validates their work by performing tests and applying its professional judgment to the adequacy and effectiveness of the whole process. This coordinated approach can yield several benefits.

Control Responsibility In a well-planned and designed CSA setting, the process owners assume greater responsibility in reviewing the effectiveness of controls. Moreover, the process can transfer knowledge among the owners and implementers of the processes. This also can facilitate greater synergy between process owners and the process implementers and increase input from business units about their activities through a participative approach.

Control Improvement With internal audit's assistance in facilitating the CSA effort, the business units can review the process flow together with evaluation of control effectiveness and compare them to best-case scenarios based on industry benchmarks. This can assist in greater information flow among the business units, facilitate soft controls such as monitoring, and enable continuous improvement.

Information Gathering Through enhanced level of understanding of

Soft controls are a component of internal audits of culture and behavior, according to the KPMG article, "Culture and Internal Audit: Why Soft Controls Make a Difference."

THE CSA MATRIX

Internal auditors facilitating a CSA should ask pertinent questions to solicit responses about the effectiveness of soft controls. While there is no standard list of questions, internal auditors could develop questions with input from management and work teams. Depending on the nature and importance of the questions, internal auditors can assign them weighted scores and calculate the final score using the number of employees that provided the response. The two examples below illustrate how a matrix can help the CSA assess the soft controls related to ethics policy and staff motivation.

EXAMPLE 1

Question: Does the organization have an effective ethics policy?

	There is an ethics policy in your organization. Are you aware of it? (Yes/No)	Did you receive any training in policies and procedures associated with ethics management in your organization? (Yes/No)	Do you think the current arrangements for enforcement and penalties are adequate? (Yes/No)
Weighting	*(30)*	*(30)*	*(40)*
Employee Responses			

EXAMPLE 2

Question: Are you adequately motivated to do your job?

	Do you personally feel equipped with the required knowledge and skills to do your job? (Yes/No)	Do you have a well-defined quantity and quality of goals? (Yes/No)	Do you feel encouraged that you can discuss innovative and better ways of doing business in your unit? (Yes/No)
Weighting	*(30)*	*(30)*	*(40)*
Employee Responses			

the client's activities, a CSA can assist the internal audit activity in gathering useful and validated information from the workshops. These inputs could assist internal audit in better planning its use of resources to focus on significant control weaknesses. Moreover, they can help auditors forge greater collaboration with the operating managers and work teams.

Management Involvement By encouraging control consciousness, CSA can increase management's participation and assumption of responsibility for risk management and control processes. Additionally, management can use the CSA forums to clarify its objectives and the ways through which the identified risks are addressed to achieve the organization's objectives.

SOFT CONTROL TESTING

While there is no one best approach to conducting a CSA, internal audit clients typically choose to perform facilitated team workshops, surveys, or management analysis of selected business processes, risk management activities, and control procedures.

As facilitators, internal auditors can assist the work teams in interlacing the questions for testing the soft controls together with the tests for hard controls. While there is no standard list of questions that fits every organization, the CSA facilitators could work with operations managers and work teams to ask open questions that could provide information about key issues using techniques such as surveys, interviews, games, and behavioral observation.

The questions could focus on themes such as management's commitment to fraud risk management,

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

management's working style, employees' motivation, communication and sharing of information among members of work teams and management, and the integrity and ethics of employees. CSA workshops can enhance participating employees' awareness and acceptance of soft controls, because those who perform the tasks are in a better position to appreciate the strengths and weaknesses of the controls, particularly the informal aspects of controls. However, auditors should ensure their questions are framed in consideration of the controls that address behavior and culture. Additionally, they should administer these questions in a mutually motivating and trustworthy environment.

Above all, testing soft controls demands specific interviewing skills such as active listening, empathy, and motivation. For the purpose of their assessments, the CSA team can construct a matrix that considers the issues being tested (see "The CSA Matrix" on page 59).

A well-planned CSA can overcome the limitations of traditional audit techniques in assessing attitudinal issues.

VALIDATION OF RESULTS

Because the information obtained during the CSA workshops and interviews is verbal information, internal auditors must validate this evidence to assess the controls. Validation of results is necessary because the information gathered during a CSA may not have the same attributes as evidence internal auditors would obtain through its own testing, observation, and walk-through procedures.

Internal audit should plan its validation procedures in advance, including determining the people who will be involved and the extent of validation needed. The degree of quality and quantity of validation helps in determining the type of audit to be undertaken in consideration of the organization's culture and the extent of testing to be performed.

Some validation procedures include validating the CSA results with past audit results over the control activities, reviewing the appropriateness of action taken in cases involving violation of the organization's code of ethics, and in case of sensitive information, discussing and validating the results by the chief audit executive at the appropriate level of senior management. Moreover, auditors should bear in mind the local values, culture, and practices in determining the type of validation procedures to be followed.

THE WAY FORWARD

Despite its benefits, CSA can be challenging to successfully implement in an organization. Internal audit may face:

- Lack of management support in setting the tone of the CSA.
- Lack of clarity about the roles and responsibilities of participants in the CSA process and its expected benefits in a formal document.
- Disinterested or skeptical staff.
- Rigid and complex organizational culture and structure that do not facilitate the free flow of ideas and information.
- Management's inaction on the action plan developed through the CSA process, which could result in resentment and negative feelings among employees.

To ensure that the process will not be counterproductive, the entities planning to undertake CSA should take adequate precautions. They should identify the appropriate format for CSA, such as workshops or surveys, that would facilitate open and candid communications in the CSA process. Additionally, they should review and document the expected value out of the CSA process and create control awareness by educating the staff through focus group discussions and workshops. Senior management should be involved in planning and designing the CSA process.

Undertaking a pilot study of the CSA process for one selected process/business unit can yield lessons that can be applied to future CSA initiatives. Finally, internal audit should follow up the planning phase and the results of the CSA by conducting an independent validation.

Through its collaborative approach that promotes self-assessment, CSA provides an opportunity for management, work teams, and internal auditors to meet the challenges in assessing the effectiveness of soft controls. For example, a well-planned CSA can overcome the limitations of traditional audit techniques in assessing the attitudinal issues that confront people when they are pursuing organizational objectives. Such insights could make it easier for management to buy in to the results of self-assessments when they reveal weaknesses in soft controls. Better still, addressing those weaknesses could help internal audit reduce the likelihood of repeat findings in the future. Ia

ISRAEL SADU, PHD, CIA, CRMA, CISA, *is an auditor with the United Nations Office of Internal Oversight Services in Amman, Jordan.*

BY DAWNELLA J. JOHNSON + GARY E. PETERSON EDITED BY MARK BRINKLEY

THE CORPORATE GOVERNANCE AUDIT

All organizations can benefit from strong governance oversight, with an assessment led by internal audit.

All too often and too easily, corporate governance is evaluated and measured simply by reviewing the structures and processes that an organization implements to achieve lofty ethical principles. However, assessing the effectiveness of governance requires more than reviewing how frequently a board meets, the number of committees an organization may maintain, the language in a code of ethics, or the aspirational pronouncements from the CEO's office. Evaluating the effectiveness of governance is, at its core, a continuous process of reviewing and measuring behaviors. Such an assessment begins with understanding an organization's business strategy and culture.

Ideally, organizations have a business strategy and an aligned business culture. The business culture is a set of risk practices and behaviors that are critical to the success of the business strategy. Accepted risk practices might be driven by the elements of the strategy itself—such as quick decisions, rapid growth, and speed to market—or they might be requested by shareholders concerned with capital preservation and adherence to risk appetite. Third parties, such as regulators interested in compliance, or accepted industry practices, such as fair dealing, also can shape accepted risk practices.

Good governance provides the oversight to ensure behaviors, however sourced, remain within accepted risk parameters. An effective governance program sets boundaries against conduct that might cause undue risk or ethical impairment to the business strategy, and it includes measurable tools to reward conduct within the accepted culture. Just as business strategies vary, so too do governance oversight models.

A good starting point when evaluating the scope and efficacy of a governance program is to review the organization's enterprise risk management (ERM) framework. Ideally, the organization will have already identified significant inherent risks in a variety of disciplines, including market, strategy, reputation, operations, technology, law and compliance, and human resources. This risk analysis provides a solid indicator as to the scope, type, and level of governance oversight required.

The effectiveness of a governance program is best measured in terms of the level of adherence to accepted behaviors. In making this determination, some specific areas to review include: strategy and governance alignment; focused messaging; and measurement, accountability, and consequences.

Strategy and Governance Alignment A first step in examining the effectiveness of governance is to review the fundamental alignment of

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

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

the organization's business strategy and culture with the governance oversight model and framework. The type, level, nature (such as proactive or reactive), and scope of the overall governance program should be commensurate with the business strategy and culture. For example, organizations with hard-driving business strategies often require cultures that "push the envelope" on risk taking. What behaviors does the organization require and reward to accomplish its business strategy? High sales levels? Rapid revenue growth? Continuous product introduction? This type of aggressive strategy and culture can result in a substantial level of organizational risk. In such a case, the internal auditor would expect to see a high level of proactive governance oversight in terms of structures, regular reporting on the quality and effectiveness of internal controls, multiple communication channels and issue-escalation paths, scenario-based staff training, and a robust reporting structure to capture potentially adverse behaviors and risks.

Consider an example in financial services. Wells Fargo's high-risk business strategy was based on rapid and substantial customer fee growth and tied staff compensation to numbers of accounts created. This strategy carried the obvious inherent risk of bogus account creation, which, indeed, occurred. Employees created an estimated 3.5 million false customer accounts. From the outset, this high-risk strategy should have demanded proactive attention to protect the organization and its customers. Ultimately, the lack of a targeted level of governance oversight had dramatic, negative consequences.

Focused Messaging Sound governance requires a clear articulation of the acceptable (and unacceptable) behaviors necessary for accomplishing the business strategy. Senior management is responsible for clearly articulating expected behaviors and verifying the governance structures that effectively carry this message throughout the organization.

For this reason, the content, level, and quality of the messaging should be reviewed. The messaging should speak to the inherent high-risk areas identified in the ERM framework and provide direction for issue identification, escalation, and resolution. The internal auditor should determine how the messaging is communicated throughout the organization. The auditor also should consider the size and scope of the organization as, especially in the case of large organizations, it is important that the message resonates across wide geographic boundaries, languages, and customs.

Measurement, Accountability, and Consequences While the determination of the business strategy and culture, the governance framework, and the articulated message of acceptable behaviors come from the top down, the determination of the effectiveness of the governance program is best seen in the measurement of behaviors. In other words, measuring effectiveness is a "bottom-up" exercise.

Behavior measurement is not as difficult as one might expect. Behaviors that result in adverse risk taking, lawsuits, fines and penalties, fraudulent or illegal actions, or a wide range of discriminatory or unethical practices generally are tracked and reported. Issues involved in job performance often are tracked in the organization's performance evaluation system. The reviewer should determine whether the organization has compared the adverse events that are reported to the criteria of acceptable risk and ethical behaviors to improve the governance platform. Questions to consider include:

- Has the organization determined where gaps and vulnerabilities have occurred?
- Has the organization used the results to determine how proactive the governance system has been?
- Have potentially damaging issues been escalated for remediation?
- Have certain categories of adverse behavior decreased?
- Have new controls or training been implemented in significant areas of risk and conduct?
- Has the organization identified geographic areas in which the governance program operates better than others?
- Have the risk issues correlated to those delineated in the organization's ERM framework?

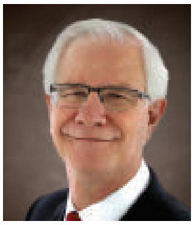
In assessing the sustainability of a governance framework, internal audit should look for two ingredients: accountability and consequence. Were instances of adverse behavior subject to both personal accountability and appropriate consequence? Employees quickly know when adverse behavior goes unpunished or when responsibility for such behavior is not acknowledged. Adverse behavior for which there is no accountability results in lack of confidence in the integrity of the governance program, and, ultimately, it impairs program sustainability.

Internal audit also should evaluate the reward framework: Does the governance program reinforce appropriate behavior via a reward system? Organizations in which exemplary behaviors are rewarded are characterized by a governance framework that shows strength and sustainability.

Every business has its own culture and goals and, therefore, its own risk comfort levels. All businesses can benefit from a strong governance oversight program, with an assessment led by internal audit. An evaluation of governance effectiveness should address not only structure, but also the alignment among strategy, culture, and measurable behaviors. Ia

DAWNELLA J. JOHNSON *is a partner at Crowe Horwath LLP and the global leader of its internal audit practice in New York.*
GARY E. PETERSON *is a managing director at Crowe Horwath in New York.*

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



BY J. MICHAEL JACKA

PROFESSIONALISM ABOVE ALL ELSE

Auditors must aim for high standards of behavior, even when stakeholders don't reciprocate.

Recently, I've been talking to anyone who will listen about the role of internal audit policies, procedures, and standards, and how they impact the success of both the profession and individual departments. Although I believe all such guidance is fundamental to audit effectiveness, I contend that the foundation for our success is really composed of three basic rules—by focusing on them, all other policies, procedures, and standards become even more effective.

The first rule comes from the Hippocratic oath: "Do no harm." The second is taken from the Nordstrom Employee Handbook's single instruction: "Use your good judgment in all situations." And the third is one that I just felt needed to be added: "Do all of this with your brain somewhere nearby." Together, these rules cover the areas of ethics, critical thinking, and common sense. I think they embody much of what internal audit strives to achieve in its strategies, in its planning, and in its day-to-day activities.

Recently, while I was discussing these concepts with a colleague, he argued that they would only work if our stakeholders followed the same principles. He seemed to be inferring that we should only treat others with the fullest of respect when we are similarly respected. I cannot disagree more.

I have a recurring conversation with my kids where I ask why he or she (I have one of each) is behaving a certain way toward the other. Generally, each one tells me that the other treats him or her in a similar fashion. I try to explain that, if either were willing to behave differently, the other might respond in kind. I am trying my best to send a message: Model the positive action that is desired, not the negative action of others.

In response, I get a look that every dad in the world knows—the "don't be so stupid" look. (At this point I am loathe to point out that my kids are 28 and 30 years old. Sigh.)

It is not internal audit's responsibility to model the specific behaviors of its stakeholders; it is internal audit's responsibility to exemplify professionalism in all it does. We have to approach our work with the intent of doing no harm. We have to use good judgment, rather than follow meaningless rules and procedures, in all we do. And we have to use common sense at all times.

Internal auditors must set higher standards of behavior, rather than fall into the trap of lowering ourselves by practicing the poor behaviors of others. We have to act as professionals, no matter how unprofessionally we may be treated.

I have yet to see a situation where being a professional, even in the face of the most unprofessional behavior by the highest levels in the organization, did not work to the benefit of the department and of the organization as a whole. 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

DIVERSITY AND INCLUSION IN TODAY'S BUSINESS

Is your organization a reflection of your values?

SUE TOWNSEN
Chief Diversity Officer
KPMG LLP

SHARON WHITTLE
Principal - Human Capital Services
Grant Thornton

Why should CEOs and boards be concerned with diversity and inclusion?

WHITTLE Why wouldn't they be concerned about diversity and inclusion? We have a diverse world and a diverse talent pool. Many studies have shown that diverse teams perform better, and for teams to be successful, they must have diversity of thought, not just visible diversity. If you're a business owner or CEO, and you consider who your customers or clients are, you should recognize that they're a very diverse population. Therefore, having diversity among leaders and among teams helps you better serve them as you can better tailor your products or solutions to meet their specific needs. Customers and clients also can look to companies and say, "Am I doing business with a company that respects diversity and inclusion, and that looks like me or my company?"

TOWNSEN Inclusion and diversity are both critical talent and business issues. To be an employer of choice, and to have fully engaged employees, you need a genuinely inclusive culture. Feelings of exclusion lower productivity in employees and increase turnover. Inclusion can unlock the power of diverse teams, bringing different perspectives and helping to drive innovation. In addition, the demographics of our country have changed. To get the best, you need to be hiring the best. Stakeholders, customers, and clients also are demanding it. Customers are diverse and companies need the best thinking to help solve complex business challenges or identify new market opportunities.

What should a diversity/inclusion program include?

TOWNSEN Organizations should concentrate on three main areas to be successful. First is driving inclusion in a company's culture. Inclusive behaviors should be developed in all leaders who, in turn, are accountable for demonstrating those behaviors. Second is to focus on key human resources processes, including talent acquisition, development, and performance management. Together with a strong diversity recruiting strategy, it's important to mitigate any potential bias in these processes. Finally, organizations need vibrant, inclusive networks with defined objectives. This is where connectivity happens. People stay when they feel they belong. Networks can be designed to help drive development of diverse professionals, provide networking opportunities, and encourage retention. They provide safe places for groups to discuss challenges. Networks also can be instrumental in connecting with clients and the larger community. When all is said and done, a relentless focus on measurement and governance helps ensure that defined objectives are being met.

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

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

WHITTLE Determining the pieces of a diversity and inclusion program will depend on where the organization is in its evolution of a diversity and inclusion strategy, what its culture and values are, how its approach to diversity aligns with that, and how it is going to measure its progress. At Grant Thornton, diversity and inclusion is an imperative, and it's embedded in our culture. They are embedded in not only every aspect of the talent life cycle, but also in the client experience, as well as our involvement in the community.

What if the organization doesn't have a program?

WHITTLE First and foremost, if you don't have a program you should be examining "why?" Start with your organization's vision and values. Do your current vision and values support having a program? Or, do you need to rethink them? Vision and values drive culture, which forms the true foundation of the organization. Think about the potential impact of a program on your organization's stakeholders.

TOWNSEN It isn't about a program, it is about whether it is a business imperative. If it is, companies must approach diversity and inclusion as a strategic priority and put appropriate resources behind it. There are many avenues to get support to develop an approach, but the first step is understanding and communicating the business case to the organization.

What should be included in a diversity/inclusion audit?

TOWNSEN From an audit perspective, some of the key lenses include strategy and governance, regulatory, and process. A few considerations include: Is there a clearly defined diversity and inclusion strategy? Are the appropriate stakeholders involved and being held accountable? Are results measured? Another approach to consider is to audit talent processes to assess for unconscious bias. For example, organizations can look at performance ratings and promotion rates of diverse talent compared to nondiverse talent to uncover insights.

WHITTLE Metrics that should be in an audit include recruiting, hiring, retention, promotion pattern, training and development, succession planning, mentoring and coaching, and leadership development. There are other issues that should be considered. Is there a communications plan for how executives and others will communicate with the rest of the organization? Is there a diversity statement? Are there measurable goals? Is leadership united and consistent in its level of program support? Audits should be conducted across multiple geographies and countries, business lines, and divisions to determine the level of consistency. Defining accountability also is important. Accountability for these programs should be defined in writing in job descriptions, performance evaluations, and promotional goals. Accountability can drive the experience so that stakeholders wake up every day and live it.

How should internal audit approach diversity/inclusion within its own ranks?

WHITTLE In the same way diversity and inclusion is important for diverse teams, it's equally important in internal audit. Some studies on brain science, particularly around gender, and how men and women approach problems differently, provide additional evidence for having diversity and a complete spectrum of skills for teams to be successful. The ability to have people on a team who think differently and are willing to challenge each other is vital. Internal audit is about asking the right questions and being skeptical and willing to challenge. It's difficult to achieve that if you don't have a diverse group of individuals working together who have very different ideas.

TOWNSEN No differently—internal audit is just like any other function. There's value in diversity and working together, particularly in harnessing unique perspectives to add value and find solutions.

How does your company approach diversity/inclusion?

TOWNSEN We are proud of our inclusive culture at KPMG. For us, this means our people feel free to bring their full, authentic selves to work every day and share ideas and passions in ways that enrich our teams, spur innovation, and drive the firm's success. Our commitment to inclusion and diversity influences everything we do, including the way we recruit, train, and develop our people. To continually strengthen our workforce and impact, we established several strategic priorities that include driving increased diversity, instilling inclusive leadership, and developing next-generation leaders at KPMG and beyond. At every level, our people take ownership for creating an inclusive culture—leading and inspiring our teams, enabled by a framework of national diversity advisory boards, local networks, and inclusion councils. Together, we help create an environment of dialogue and action, addressing the challenges and capturing opportunities that matter most to our firm, our clients, and our communities.

WHITTLE We approach diversity and inclusion as part of our culture and a key part of who we are. We look not only at someone's outward, or visible diversity, but also at someone's diversity of thought, background, and experience. Those characteristics carry so much importance. Our strategy also includes measuring and assessing certain retention, advancement, and promotion statistics. We've also placed importance on education, skill building, and leadership as well as benefits and work-life flexibility. For us, it's about employee engagement and being able to advance diverse groups within the organization. One example is being able to advance more women into leadership roles within our firm. Ia

IIA Calendar

IIA CONFERENCES

www.theiia.org/conferences

OCT. 30–NOV. 1
All Star Conference
Bellagio Hotel
Las Vegas

MARCH 12–14, 2018
General Audit Management Conference
Aria Resort & Casino
Las Vegas

MAY 6–9, 2018
International Conference
Dubai World Trade Centre
Dubai, UAE

IIA TRAINING

www.theiia.org/training

OCT. 17–20
Various Courses
Washington, D.C.

OCT. 17–21
Operational Auditing: Influencing Positive Change
Online

OCT. 23–25
Vision University
Toronto

OCT. 23–27
Various Courses
San Diego

NOV. 1–27
CIA Learning System
Comprehensive
Instructor-led Course
Part 3
Online

NOV. 7–10
Various Courses
Chicago

NOV. 7–16
Audit Report Writing
Online

NOV. 13–15
Vision University
Chicago

NOV. 14–17
Various Courses
Las Vegas

NOV. 20–21
IT General Controls
Online

NOV. 27–DEC. 15
CIA Learning System
Comprehensive
Instructor-led Course
Part 1
Online

NOV. 29–30
Data Analysis for Internal Auditors
Online

DEC. 4–13
Fundamentals of IT Auditing
Online

DEC. 5–8
Various Courses
Denver

DEC. 5–8
Various Courses
New York

DEC. 5–14
Lean Six Sigma Tools for Internal Audit Planning
Online

DEC. 6–15
Assessing Risk: Ensuring Internal Audit's Value
Online

DEC. 11–14
Various Courses
Orlando

DEC. 12–15
Various Courses
Austin, TX

DEC. 18
Fundamentals of IT Auditing
Online

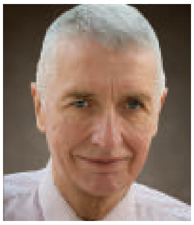
DEC. 19–20
Succession Planning: Leveraging and Influencing Millennials and Other Generations
Online

BER/NOVEMBER/DE

THE IIA OFFERS many learning opportunities throughout the year. For complete listings visit: www.theiia.org/events

PHOTO: RAWPIXEL.COM / SHUTTERSTOCK.COM

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



BY IAN DOUGLAS

INFLUENCE, DON'T ANTAGONIZE

The right language can make all the difference in an audit report.

Inexperienced audit staff members often believe they need to justify their existence by identifying major issues on engagements. Seeking to make an impression, they may use excessively critical or even sensational language, with no regard for diplomacy. This approach, while attention-getting, generally does not foster constructive dialogue or prove helpful to the client. Auditors must be conscious of reporting accuracy, but they also need to consider how their reports might impact the recipient.

Even when clients work hard to manage risks, internal auditors may still identify significant weaknesses or deficiencies in their area. When reports are worded carelessly, clients may interpret the content as adversarial, unfair, or hurtful, eliciting a defensive and negative response. Moreover, a critical report can have career-damaging consequences, even leading to dismissal.

Instead of a combative approach, internal auditors should consider a balanced, constructive reporting style, reserving strongly critical language for situations where evidence of negligence or incompetence exists. Facts can be colored by the way they are expressed—something that politicians and public relations experts have long realized. Auditors, too, should be mindful of the consequences their words can have.

Consider an observation that might be perceived as unnecessarily critical: "A review of customers' complaints revealed that 28.9 percent of complaints were from customers annoyed by the heavy-handed and bureaucratic requirements for evidence of purchase before a refund was made." Alternatively, the same observation could be expressed less judgmentally: "A review of customer complaints revealed that 28.9 percent of complaints were from customers experiencing difficulties in complying with the department's requirements for evidence of purchase before a refund was made." In both versions, the basic facts are the same—but the tone between them differs significantly.

Using harsh language, even if unintentional, can often be counterproductive, making clients less open to implementing changes. Of course, some situations merit a highly critical report, but even then auditors should consider whether the language used might be overcritical.

If the internal auditor's objective is to achieve beneficial change, a balanced, constructive approach to findings and recommendations offers the best option. Softened language does not weaken the report or let management "off the hook," especially if supported by a robust approach to follow-up of agreed recommendations to confirm implementation. Audit communications should be clear and honest, and report writers should not shy away from legitimate, justified criticism.

Internal auditors must choose their reporting language carefully, avoiding language that ultimately may undermine their efforts. Practitioners should place themselves in the client's shoes and, ideally, use language that they themselves might want to hear. Ia

IAN DOUGLAS *is a retired head of audit and an elected Fellow of the Chartered Institute of Internal Auditors. He is author of the book,* Writing Reports That Get Results.

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