Ia
INTERNAL AUDITOR

JUNE 2019

A PUBLICATION OF THE IIA

A Risk Management Case Study

North American Board Chair:
It's Time to Step Forward

Thwarting Bias in AI

The Audit Committee
Ethics Expert

THE CLEAR CHOICE

Mounting evidence shows better business performance for organizations that choose an ethical path.

GRC
CONFERENCE 2019
Aug. 12-14 | Ft. Lauderdale, FL, USA

GRC 2019 Program Is Aligning for Impact

The IIA and ISACA are excited to once again partner to bring you "THE" event for governance, risk, and control! This year will feature two thought-provoking professional leaders to open and close the conference:

Patrick Schwerdtfeger
Business Futurist

Embracing Disruptive Innovation

Simon T. Bailey
Executive Advisor, Career Mentor, Author

Shift Your Brilliance — Leading Amidst Change and Uncertainty

GRC 2018 sold out, so don't wait — register now for GRC 2019 and save $200!

www.theiia.org/GRC

ISACA®

The Institute of Internal Auditors

Ia
INTERNAL AUDITOR

JUNE 2019 VOLUME LXXVI: III

FEATURES

FOR THE LATEST AUDIT-RELATED HEADLINES visit InternalAuditor.org

Ia
INTERNAL AUDITOR

JUNE 2019 VOLUME LXXVI: III

DEPARTMENTS

PRACTICES

INSIGHTS

ONLINE InternalAuditor.org

Getting a Handle on Harassment What's considered appropriate behavior in the workplace is continuing to evolve. Organizations need to respond to the changes and ensure employee protection.

Assessing AI Initiatives In our latest video series, Brian Foster, Microsoft general manager, Internal Audit, walks through the challenges of auditing AI.

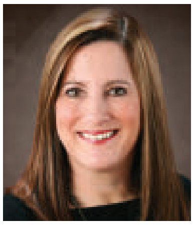
Crime's Digital Transformation Fraudsters and cybercriminals are bringing innovation to wrongdoing, harnessing mobile digital platforms and advanced techologies to commit disruptive crimes.

Fuel for Fraud A recent case underscores ongoing fraudulent activity in biofuel subsidy and compliance credit programs.

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 © 2019 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.

COVER AND PREVIOUS PAGE: ILLUSTRATION BY SEAN YATES, BASE PHOTOGRAPH BY KONSTANTTIN / SHUTTERSTOCK.COM; THIS PAGE, TOP: ALEXDNDZ / SHUTTERSTOCK.COM, BOTTOM: BAONA / I-STOCK.COM



CULTURE, ENGAGEMENT, AND BUSINESS SUCCESS

In a recent article on Gallup's website, "3 Daily Actions That Set the Tone for Workplace Culture," author Craig Kamins writes, "Some workplace cultures motivate employees and fuel performance." Others, he says, "drain employees' motivation and make employees feel as though they have no control over their environment nor an incentive to perform."

According to Kamins, employees' perceptions about their work culture hinge on their leaders' words and actions. Three daily behaviors that set the tone for the workplace culture, he writes, and lay the "groundwork for exceptional engagement," are:

1. Be respectful toward employees.
2. Communicate what is happening in the organization.
3. Promote accountability and fairness.

A few years ago, The IIA's chief marketing officer, Monica Griffin, took on the responsibility of addressing The Institute's corporate culture. As the organization grew and evolved, it was a task that was long overdue. She and her working group, of which internal audit was a part, identified cultural challenges and developed The IIA's core values:

- Put Our Members First
- Do the Right Thing
- Commit to Shared Success
- Work Smart

Today, staff—from the top down—are measured by how well we adopt these values. They are part of our annual performance review, and we are recognized for exhibiting them. After all, by engaging in these behaviors we better serve our members, which enhances The IIA's reputation and business performance.

In this issue of *Internal Auditor*, we examine organizational culture from multiple angles and consider internal audit's role in helping ensure it remains healthy. Our cover story, "The Right Path" (on page 24), considers how an organization's ethical culture affects its bottom line. The new IIA North American Board chair, Benito Ybarra, says it is part of internal audit's job to help drive an effective corporate culture (see "Step Forward" on page 36). In "Board Perspectives" (on page 56), author Matt Kelly asks, "If society wants corporations to exercise a sharper sense of ethics and moral responsibility, do we need more ethics and compliance officers serving on boards?" Plus "Eye on Business" (on page 60) considers what it takes to assess, monitor, and report on the organization's culture. And don't forget to visit InternalAuditor.org and read Jim Roth's ongoing series on culture.

When it comes to organizational culture, we've got you covered.

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
APRIL 2019
A PUBLICATION OF THE IIA
Auditing Risk's Upside
Smart Cities Present Steep Audit Challenges
Keep Your Focus on the Client
Navigating Stakeholder Expectations
GDPR's GLOBAL REACH
The philosophy underlying Europe's data privacy law is finding its way into regulations around the world.

Proactively Address Risk

What I have found in my experience on risk committees is that executive managers are often hesitant to report emerging risks not clearly affecting their company today, unless they can show proactive actions or treatments. For many executives, merely saying they are monitoring the trend or direction of the potential event or risk is not enough, and they defer discussions at the board or audit committee levels.

I find this fear limits the value of risk governance and diminishes the real need for management to be constantly monitoring their risk landscape and giving that comfort to the board. In fact, sharing a risk insight might be appreciated and more impressive to the board than sweeping it under the rug. I guess culture eats risk management for lunch!

MICHAEL LYNN *comments on "Anticipating Surprises" ("Update," April 2019) on LinkedIn.*

Outside of College Control

College admissions is a very complicated process with many moving parts. Art Stewart's lesson learned about setting, monitoring, and enforcing clear standards for the role of admissions consultant and essay-writing services is outside the control of a school's admission department. We have no control over parents hiring admission consultants and have no way to enforce it. Also, his lesson learned about a review of how applicant documentation and testing is conducted is also partially outside the control of the college or university. The colleges/universities are not the ones administering or proctoring the ACT or SAT—the colleges/universities just get the test scores. It is ACT's and SAT's responsibility to check a student's proof of identification.

ANONYMOUS *comments on Art Stewart's "Big Scam on Campus" (InternalAuditor.org).*

Maintain Independence

The risk management function must be an integral part of any transformation project. However, the internal audit function should only be involved to the extent the principle of independence is not compromised.

MANU VARGHESE *comments on Tim McCollum's "Fit for Digital" (InternalAuditor.org) on LinkedIn.*

Audit Report Attention

Thanks for bringing to our attention the audit report errors. Most of the time we are focused only on fulfilling requirements and sometimes we make mistakes. It is helpful to recognize where we should pay twice the amount of attention in our reporting.

ALBANA GJINOPULLI *comments on the video, "Common Audit Reporting Mistakes" (InternalAuditor.org), on LinkedIn.*

Ia
INTERNAL AUDITOR
JUNE 2019
VOLUME LXXVI:III

EDITOR IN CHIEF
Anne Millage

MANAGING EDITOR
David Salierno

ASSOCIATE MANAGING EDITOR
Tim McCollum

SENIOR EDITOR
Shannon Steffee

ART DIRECTION
Yacinski Design

PRODUCTION MANAGER
Gretchen Gorfine

CONTRIBUTING EDITORS
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, FCPA, FCGA, FCMA
Andrew Bowman, CPA, CFE, CISA
Mark Brinkley, CIA, CFSA, CRMA
Robin Altia Brown
Adil Buhariwalla, CIA, CRMA, CFE, FCA
Wade Cassels, CIA, CCSA, CRMA, CFE
Faizal Chaudhury, CPA, CGMA
Michael Cox, FIIA(NZ), AT
Haylee Deniston, CPA
Kayla Flanders, CIA, CRMA
James Fox, CIA, CFE
Michael Garvey, CIA
Jorge Gonzalez, CIA, CISA
Nancy Haig, CIA, CFE, CCSA, CRMA
Daniel Helming, CIA, CPA
Karin L. Hill, CIA, CGAP, CRMA
J. Michael Jacka, CIA, CPCU, CFE, CPA
Sandra Kasahara, CIA, CPA
Michael Levy, CIA, CRMA, CISA, CISSP
Merek Lipson, CIA
Thomas Luccock, CIA, CPA
Michael Marinaccio, CIA
Alyssa G. Martin, CPA
Dennis McGuffie, CPA
Stephen Minder, CIA
Rick Neisser, CIA, CISA, CLU, CPCU
Hans Nieuwlands, CIA, RA, CCSA, CGAP
Manish Pathak, CA
Bryant Richards, CIA, CRMA
Jeffrey Ridley, CIA, FCIS, FIIA
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
Stephen Tiley, CIA
Robert Venczel, CIA, CRMA, CISA
David Weiss, CIA
Scott White, CIA, CFSA, CRMA
Rodney Wright, CIA, CPA, CFSA
Benito Ybarra, CIA

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

IIA CHAIRMAN OF THE BOARD
Naohiro Mouri, CIA, CPA

PUBLISHED BY THE INSTITUTE OF INTERNAL AUDITORS INC.

CONTACT INFORMATION

ADVERTISING
sales@theiia.org
+1-407-937-1388; 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")

2019-2589

Reviewing the three lines of defense... AI's positive environmental impact... The CIA exam gets an upgrade... Organizations enhance ethics safeguards.

Update

FRAUGHT WITH CORRUPTION

In a worldwide ranking, three industries presented the highest levels of corruption risk.

1 Construction and development

2 Infrastructure

3 Oil and gas

Source: The Risk Advisory Group, Corruption Challenges Index 2019

PRIVACY COMPLIANCE A TOP RISK

Global privacy regulations are creating a complicated path for organizations.

Accelerating privacy regulation has surpassed talent shortages as the top emerging risk in Gartner Inc.'s 2019 Q1 Emerging Risks Monitor Report. The global survey notes privacy regulation was a top risk for at least 70% of senior audit, compliance, finance, and risk executives in four sectors: banking, financial services, technology and telecommunications, and food/beverage/consumer goods.

"With the General Data Protection Regulation (GDPR) now in effect, executives realize that complying with privacy regulations is more complex and costly than first anticipated," says Matt Shinkman, managing vice president and risk practice leader at Gartner, a global research firm. Adding another layer of complexity for companies to navigate privacy regulation is the California Consumer Privacy Act, set to take effect in 2020.

Accelerating privacy regulation also is a "very rapid velocity" risk that will have high organizational impact if it materializes. Executives view it as a concrete threat to their organizations, ranking it the highest-probability risk of any of the top 10 in the report. Executives' GDPR-specific concerns are evolving into "a broader recognition that their organizations need to overhaul their

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

IMAGES: TOP, ALEXDNDZ / SHUTTERSTOCK.COM; LEFT, MALERAPASO / I-STOCK.COM

entire data security governance strategies," Shinkman says.

In line with the results of the Emerging Risks Monitoring Report, Gartner's 2019 Privacy Program Priorities survey found that the top priority of privacy executives is adapting to a volatile regulatory environment. About four in 10 are confident in their current abilities to keep pace with new requirements. Establishing a privacy strategy to support digital transformation and implementing an effective third-party risk management program are the No. 2 and No. 3 priorities, respectively. **—S. STEFFEE**

3 LINES IN REVISION

The IIA reviews the relevance of the risk management model.

The IIA is reviewing the widely accepted Three Lines of Defense model with the aim of ensuring the guidance is more applicable to today's changing organizational environment. The review seeks to clarify essential responsibilities in governance, risk management, and control. The Institute will be seeking public comment on its website.

The IIA's Three Lines of Defense task force seeks to "breathe new life" into the model by focusing on organizational success and embracing governance processes. IIA Global Chairman Naohiro Mouri explains that The IIA recognizes that risk "goes beyond 'defense'" and can create opportunity. "We want to ensure organizations can allocate and structure their resources and responsibilities by using the Three Lines of Defense to their advantage," he says.

To that end, the review is considering both a reactive and proactive approach to fulfilling an organization's purpose and value creation. Moreover, the task force is evaluating how the model can be scaled for organizations of different sizes.

Additionally, the task force is considering how internal audit functions should address the "blurring of the lines" when they are asked to take on responsibilities within areas of the organization. The objective is to stress flexibility among the lines. Check for updates at www.theiia.org/3LOD **—T. MCCOLLUM**

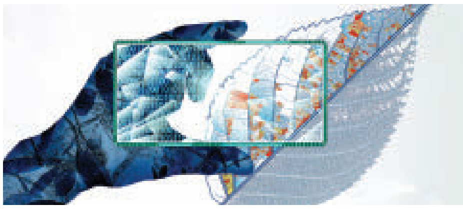
CAN ARTIFICIAL INTELLIGENCE SAVE THE WORLD?

Research suggests AI could reduce environmental impacts and raise economic growth.

Here is some good news about artificial intelligence (AI): It might help save the environment. A PwC report forecasts that applying AI to environmental management could reduce global greenhouse gas (GHG) emissions by as much as 4% in 2030.

Doing so may be good for the economy, too. Environmental applications of AI could add $5.2 trillion to the global economy by 2030 and create more than 38 million new jobs, according to the Microsoft-sponsored report.

Researchers used modeling to compare the



potential benefits of AI-based environmental applications versus continuing

NEARLY 75% OF ASIA-PACIFIC (APAC) BANKS expect fraud cases in their country to increase moderately or significantly in 2019.

MORE THAN 50% OF APAC BANKS PRIORITIZE RISK management over customer service, blocking cards on the first fraud alert.

"While protection against fraud is important, some banks are still struggling to balance prevention with customer convenience," says Dan McConaghy, president of FICO in Asia Pacific.

Source: FICO 2019 Asia Pacific Fraud Forum survey

IMAGES: TOP, MEHMETBUMA / ISTOCK.COM; RIGHT, YUUJI / ISTOCK.COM

with current practices. "The research shows the potential of emerging technology to directly support decoupling economic growth from greenhouse gas emissions in the near and long term," says Celine Herweijer, global innovation and sustainability leader at PwC UK.

How? By applying AI and other emerging digital technologies in four sectors that currently represent 60% of GHG emissions: agriculture, energy, transport, and water resources.

For example, the agricultural sector could use AI to better monitor environmental conditions and crop yields. Meanwhile, intelligent grid systems could predict and manage energy demand and supply, the report notes. AI-based traffic prediction and autonomous vehicles could transport people and cargo more efficiently and sustainably.

Regions such as East Asia, Europe, and North America stand to see the biggest reductions in GHGs and greatest economic gains, the report predicts. This is because those regions have greater digital readiness, technology adoption, and environmental policies than other regions.

Despite AI's potential, the report cautions that AI risks surrounding bias, control, and security could pose risks to the environment. Similarly, each of the four sectors must overcome existing barriers to realize AI's full benefits. **— T. MCCOLLUM**

THE EVOLVING CIA

Certified Internal Auditor exam upgrades align it with current internal audit practices, says Lily Bi, IIA vice president of Global Certifications.

How is the 2019 Certified Internal Auditor (CIA) exam different from previous exams? The CIA exam remains the foundation for all internal audit services – operations, finance, and IT audit. The most extensive changes were made to Part Three: Business Knowledge for Internal Auditing, which has always been the most challenging because the scope was massive. It is now streamlined to focus on four areas most critical for internal auditors: business acumen, information security, IT, and financial management. Almost half of Part Three focuses on advanced technology knowledge, such as data privacy and cybersecurity, an essential for today's internal auditor.

Part One: Essentials of Internal Auditing and Part Two: Practice of Internal Auditing have been revised to more closely align with the *International Standards for the Professional Practice of Internal Auditing*. The new Part One exam assesses Attribute Standards such as the foundations of internal auditing – fraud, governance, risk management, and controls. The nature of internal audit's work is evaluating and contributing to the improvement of those areas. The new Part Two exam focuses on Performance Standards, such as managing the internal audit activity and performing internal audits.

COMPANIES SEEK ETHICAL ENHANCEMENTS

Rising scrutiny is driving compliance executives to tackle misconduct companywide.

Across industries, organizations want to get better at preventing and detecting ethical misconduct by enhancing key compliance areas, according to KPMG's 2019 CCO Survey. Nearly two-thirds of the survey's chief ethics and compliance officer (CCO) respondents identified investigations and monitoring and testing as capabilities that they most want to improve. Other areas for improvement are data analytics and regulatory change management.

The report, based on a survey of 220 U.S.-based CCOs, says heightened public and regulatory focus on ethical behavior has elevated the need for ethics and compliance leadership. It points to recent technology advances and digitization as catalysts for increased public awareness of events such as data breaches and organizational misconduct.

In light of these challenges, the report suggests auditors advise organizations on revamping investigation processes, case management, reporting, and communication. **— D. SALIERNO**

PHOTO: LEFT, DANE_MARK / I-STOCK.COM

COMPLIANCE
CHAMPION

BY DANNY FRIDMAN, DROR BAR MOSHE + DAVID GABRA

EDITED BY JAMES ROTH + WADE CASSELS

ASSESSING DATA RELIABILITY

Internal auditors can follow practical steps to ensure reports are complete and accurate.

Reports from extracted data can sometimes be misleading, which can be a problem when organizations rely on them to make critical business decisions. This is especially important for organizations subject to the U.S. Sarbanes-Oxley Act of 2002 as part of the testing process.

The U.S. Public Company Accounting Oversight Board warns that having inaccurate reports might lead to key controls deficiencies, so organizations should ensure that reports used in assessing the operation of key controls are complete and accurate. Internal auditors can easily apply tools and techniques to ensure that reports and data used for decision-making are reliable.

The Impact of Bad Data

Poor data quality is responsible for an average of $15 million per year in financial losses, according to recent Gartner research. It also is a primary reason for 40% of all business initiatives failing to achieve their targeted goals. Unreliable reports can impact:

- *Strategic Decisions*—performing mergers and acquisitions, changing organizational structure, expanding to new locations, or developing new product portfolios.
- *Operational Decisions*—costing and pricing of projects, budget-related decisions and priorities, sales forecasts, production and inventory needs, and resource requirements.
- *Financial Decisions*—financial reporting, credits and loans, invoicing, collection, and investments.
- *Regulation and Compliance*—employment labor laws, intellectual property, data privacy, and software licensing.

Start With a Risk Assessment

The first step is to perform a risk assessment to determine which reports should be subject to evaluation. This should include an assessment of the report type, impact of the report for decision-making, key control considerations, change management procedures, and access restriction.

Reports can be categorized into three main types—canned, customized, and manual. Canned reports are generated from a system where no changes have been made. Those reports usually represent low risk for completeness and accuracy. Customized reports are developed based on user needs and represent higher risk for completeness and accuracy. Manual reports are created by an end user and have not passed a formal change management process for report testing. They usually represent the highest risk.

As each report type represents a different inherent risk level, identifying the report type is crucial for

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

TO COMMENT on this article,
EMAIL the authors at danny.fridman@theiia.org

the reliability assessment, and should lead to different validation activities.

Other factors that should be considered when determining reports for testing include:

- *Data Usage.* Does the report and underlying data relate to strategic, financial, operational, or regulatory decisions?
- *Impact of the Report.* Would a mistake in the report pose a potential strategic, financial, operational, or regulatory risk to the organization?
- *Control Considerations.* Is the report used in the execution of key controls to mitigate significant risks?
- *Change Management Procedures.* How effective are the change management controls for report creation?
- *Access Restrictions.* What access restriction mechanisms—such as password or permissions—are in place?

Test for Completeness

Internal auditors need to verify the report type and understand the parameters used to generate it. Just one incorrect parameter can severely impact report reliability. Because several parameters typically are used to generate a report, the internal auditor should spend time with the report owner to understand if the parameters were correctly selected.

Next, internal auditors should check whether any exclusions have been set up at either the application user-interface level or the code level. If it's the latter, assistance from developers may be needed. Auditors also should be careful not to be fooled by the report name. A procurement report named "Total Expense for Vendors" may only show expenses that are procurement-related, but not all expenses.

Internal auditors should review several areas when testing reports for completeness.

- *Look at when the report was last modified.* Checking the last modification date can highlight whether report changes occurred.
- *Common practice is to limit what data a user can see based on user access rights profiles, which should be in line with job responsibilities.* It is critical to verify that the user generating the report provides a complete report. In many cases, the end user may be indifferent or unaware of this, so it is always advisable to approach the system owner.
- *Compare different reports that should show the same data.* Because each report is built with different logic, this is a good way to test report completeness. Compare the same information from different sources and ask different stakeholders to opine on the reasonability of the data.
- *Use the "full and false inclusion" method.* Take a sample of transactions that should or should not be in the report, and verify accordingly.
- *Verify if any manual checks or system validations prevent duplicate records.* To identify such occurrences, perform a simple but effective duplication test for a sample of data fields.
- *Review blank data fields.* Missing data is a good indicator that additional checks need to be performed.
- *When using a reporting tool, such as a business intelligence application, ensure that the latest version is being used.* Upgrades usually solve technical defects, and data-warehouse interfaces can be different.

Test Data Accuracy

In testing accuracy, internal auditors need to understand which data capture method was used, as each method has a different level of risk for data reliability: on a paper form, by users directly entering data, or by a system. It's also important that auditors recognize the type of controls over system data entry and system data input validations, such as double keying and upper and lower limits.

Other items that should be assessed by internal auditors in the testing of data accuracy include:

- *The meaning of a data field.* Internal auditors should never assume, based on the column descriptions, that they understand what the data item is.
- *The source data for key data fields.* This can be done by tracing back to identify the source data repository.
- *Reasonableness.* For example, is it reasonable that a car was rented for $2,000 a night?
- *Date fields.* Dual date format issues might adversely impact any date analysis. For example, a date in a report such as 03/05/2019 might be displayed as either March 5, 2019, or May 3, 2019, depending on the end user's regional setting.

Blind Trust

Unreliable data can negatively impact key decisions. In many cases, organizations are unaware of unreliable reports, resulting in stakeholders grappling with flawed data that, ultimately, might lead to wrong or nonoptimal choices. Unfortunately, this lack of awareness may lead many organizations to blindly trust their data, which can mean disaster. Organizations are data driven, so internal auditors must ensure that decisions are made based on complete and accurate reports. Ia

DANNY FRIDMAN, CIA, CISA, CRISC, *is head of internal audit at AMDOCS in Ra'anana, Israel.*

DROR BAR MOSHE, CIA, CPA, CFE, CISA, *is deputy head of internal audit at AMDOCS.*

DAVID GABRA, CISA, *is an internal auditor at AMDOCS.*

BY BILL BONNEY EDITED BY STEVE MAR

PEACE IN OUR TIME

Audit results shouldn't drive the IT department's strategy and priorities.

Too many organizations use internal audit results to drive priorities for the IT function, which can have a devastating effect on morale. This approach sets an example for the entire organization about how to get systems-related objectives met. Initially, this can be benign as leaders try to do the right thing and help uncover systems issues that need attention. Eventually, pointing the auditors to real or suspected issues allows them to elevate any project to the highest priority, whether it is strategic or not.

For example, a software company starved back-office systems in favor of product development. As a result, IT fell seriously behind in patching internal production systems. Because the organization was audit-driven, at the next opportunity, management pointed auditors at patching, and the inevitable findings in patch management became the flag around which any desired project was wrapped to secure new funding. Step one: Hold IT accountable for not patching that system. Step two: Secure funding to "fix IT's mess."

Allowing audits to drive strategy wastes time and money, and robs management of the audit's real value—helping management validate that it is appropriately addressing risks to business processes. When the audit becomes the key objective, performing audits becomes an essential business process on its own. This mistake creates the potential for a wildly inappropriate scope that gives the IT staff the sense that audits are never-ending and self-serving.

Fear and Loathing

These issues can lead to audit fatigue and poorly executed audit activities. Before long, management is spending its time and attention fixing problems with audits instead of fixing problems found by audits.

In another example, a large financial services company purchased a much smaller company in an adjacent but highly regulated space. As is often the case, the smaller company had a much lower profile than the larger company, but that changed once it was part of a larger organization. The new management, lacking experience as a highly regulated entity, began to ramp up audits to get ahead of the regulators. As operational requirements competed with audit requests, "just get it done" replaced "do it right." At some point in this dysfunctional downward spiral, "do whatever the auditor says to get this over with" became the strategy to end the pain.

This example provides context for the skepticism, distrust, and outright fear senior executives and IT staff members have about audits. Some worry about getting in trouble for doing something wrong. Many view the time spent on audit requests as

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

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

wasted time or busy work. The fear and distrust for audits is naturally extended to the auditors, and this leads to an "us versus them" mentality. Both sides dig in and spend more time protecting their flank than solving their problems.

Some IT departments assign auditors "handlers" to choreograph activity, coach process owners to provide guarded answers, and quickly escalate issues, causing a bottleneck within leadership. Inexperienced auditors bring poor time management skills, poorly thought-out evidence requests, and negative attitudes to audits that put everyone on guard. Auditors then spend extra time gathering overwhelming evidence of control failure, and IT staff fabricates control evidence.

In addition to driving poor decision-making when used unwisely, audits often veer off track. In such cases, people too close to the situation sometimes focus on the audit as the key objective rather than managing the business process under audit. Besides these strategic mistakes, scope creep, poor communication, distrust among teams, and inexperience can plague any project and amplify any problems with an audit because of the extra scrutiny on the outcome.

In some organizations, IT may be severely underfunded and so far behind in resolving previous audit findings that the department gets accustomed to adding the next set to its ever-expanding project list. This forces leadership to spend so much time prioritizing and re-prioritizing work that audit failure becomes the de facto driver for funding. This, more than control failures, may be the finding that the audit should reveal.

The Path to Peace

It doesn't have to be like this. When used appropriately to validate assumptions and uncover blind spots, the audit program is a crucial asset for management and plays an essential role in governance. Here are 10 tips to help internal auditors, management, and IT employees get on the right track.

Audit team The audit team can become better partners to IT by taking these steps:

- *Agree with senior leadership on the strategy and priorities of the audit program.* Establish priorities and understand where to focus audits based on the risks presented by the critical business processes.
- *Ensure each audit focuses on making the business process better, not finding problems.* Internal audit should keep this goal in mind as it sets audit objectives, determines scope, and frames findings. Always solicit recommendations for improvement from management.
- *Help the organization navigate audits and examinations by external organizations (within the limits of independence).* This is particularly important as it pertains to audit scope. For example, it's not helpful to have nonregulated businesses examined by regulators. It wastes time and exposes the organization to inappropriate jeopardy. Auditors should make sure all parties agree to the scope before the audit starts.
- *Agree up front on the criteria for identifying the required evidence.* These criteria include sample selection criteria, the duration of the assessment, and the amount of evidence required to validate each test objective.
- *Agree on the process and tools to be used for requesting and receiving the evidence.* Agree on how quickly evidence is to be gathered once requested.

Management IT management can demonstrate transparency and respect for the audit process by:

- *Avoiding assigning junior people to handle examiners or auditors.* When management tries to offload audit responsibility to the least useful resource, it almost always has a negative impact.
- *Not coaching employees on how to be coy with auditors.* Internal auditors are trained to spot inconsistency and lack of transparency. Trying to hide details from auditors is unprofessional and causes them to dig deeper in that area.

Employees IT staff members who are asked to support audit activities can establish trust by taking these steps:

- *Don't assume your competence is being questioned.* "I don't know, but let me find out for you" is a better answer than guessing.
- *Don't try to sound like a lawyer.* The best way to be understood is for employees to use the language and style that is comfortable to them. The surest way to get management's attention—and not in a good way—is to call a minor testing deviation a "material weakness."
- *The auditor is not a whistleblower hotline.* Managers should remind employees to bring internal issues to their manager or a neutral member of the management team.

Look in the Mirror

Internal auditors should ensure their organization doesn't take a dysfunctional audit approach. They should review their audit strategy to make sure it addresses business process risk, provides the necessary governance assistance to management and the board, and addresses the organization's regulatory requirements. They shouldn't let audits drive the business. Ia

BILL BONNEY *is a security evangelist, author, and consultant in San Diego, Calif. and co-founder of CISO DRG Inc.*

BY MAJA MILOSAVLJEVIC EDITED BY CHARLIE WRIGHT

HOW TO AUDIT SOCIAL MEDIA

By reviewing compliance with social policies, internal auditors can help their organizations assess risks.

In today's business world, practically every organization has a presence on social media, enabling them to reach huge numbers of customers and stakeholders globally. While enhancing sales might be the primary driver for creating a social media presence, social media has a much broader scope. It builds new relationships with customers, employees, and other stakeholders, expanding awareness about the organization and its brand. It influences customer education, engagement, and feedback. And it heightens the organization's attractiveness as an employer and strengthens its reputation.

With that broader reach comes new and different types of risks for organizations and their employees, such as reputational, dark web, and data protection risks. For internal auditors, the most relevant questions relate to aspects of how the social media presence is being managed. Organizations must develop policies covering aspects such as who in the organization has the authority to use social media, what gets communicated, and which of its stakeholders should receive the communications.

Consequently, internal auditors should invest resources to audit compliance with social media policies and guidelines. To do so, auditors need to build an adequate audit approach for the still-developing area of social media-related engagements.

Social Media Strategy

A good starting point for auditing social media is the organization's social media strategy. Actually, the first question auditors should ask is whether the organization has such a document at all. A social media strategy can help establish the general basis of the organization's governance, use, oversight, and approach. The strategy also should contain the goals the organization aims to achieve from a long-term strategic perspective, thus setting the foundation for social media implementation.

Another important strategic component that internal auditors should evaluate is the specific channels that influence the organization, including validation of links, social handles, profile and account information, mission statement for the account, and key demographics. Moreover, auditors should assess whether organizational and social media goals are aligned.

Policies and Procedures

After dealing with the organization's strategic approach, the next step is to check that the social media strategy has been written into relevant policies, procedures, guidelines, and instructions. Starting with the regulatory framework that is relevant for the organization's industry,

SEND RISK WATCH ARTICLE IDEAS to editor@theiia.org

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

internal auditors should evaluate whether policies and procedures comply with state, local, and national labor laws and protected free speech rights. Ensure that relevant documents are reviewed for consistency and approved by the appropriate experts from different parts of the organization such as senior management and the legal, risk management, and internal audit functions. Finally, the assessment should seek the perspective of the organization's employees, including those responsible for social media. One concern is whether employees have documented style guides to follow for social media posts.

Dedicated Resources

Another important aspect of auditing social media is assessing whether it has adequate resources. Once the organization decides to have a social media presence, the organization needs to dedicate employees to manage its presence and establish tools for monitoring it. Appropriate management of social media should include using tools that provide information such as mentions of the organization's name, relevant post reviews, and audience behavioral patterns.

To get an understanding of the organization's social media activities, internal auditors should search the web to identify where the organization has a presence. Additionally, identifying some of the best posts and evaluating the themes that make them popular—such as the topic, pictures, and people focus—can inform management about the relevance of those posts to customers and stakeholders.

> **Identifying key metrics can give internal auditors a basis for evaluating the performance of social media.**

Identifying key metrics can give internal auditors a basis for evaluating the performance of the current social media. This not only includes assessing the current metrics in place, but also whether there should be other or different metrics. Various social media analytics tools can help auditors simplify this step.

Roles and Responsibilities

The wide scope of influence social media could have on the organization creates the necessity to establish appropriate roles and responsibilities. It would be confusing to have all the departments posting on social media on behalf of the organization at the same time and without any alignment. Likewise, it would be confusing if any employee could provide requested feedback or reply to a comment on social media.

These issues challenge internal auditors to validate that the roles and responsibilities are documented and are clear to all employees. When it comes to security, auditors should evaluate owners of each account and review security protection measures in place such as tools for controlling passwords.

Internal Communication and Training

Considering that social media can significantly impact the organization if not managed well, organizations need relevant internal communication and training programs. Employees need to know the rules for representing the organization on social media to avoid potentially negative consequences. For these reasons, internal auditors should review social media-related communication to employees as well as the frequency of training provided.

Crisis Scenarios

Another important aspect of auditing social media is reviewing whether the organization has developed crisis scenarios and assessing how the crisis would be communicated on social media channels. Generally, a crisis creates opportunities for a wide range of miscommunication throughout the organization. Internal auditors should make sure managers and social media employees are aware that such situations might happen and have a clear plan for managing those situations.

Room for Improvement

Internal auditors can provide an independent perspective and good insight for management to consider. However, to keep up with the dynamics of social media, the organization always should look for opportunities to improve social media channels as well as the controls around their use. Employees who manage social media should coordinate with other departments within the organization and constantly evaluate new developments and topics of interest in their industry, region, and community. Internal auditors can help those employees make improvements to the structure and design of the organization's social media approach that can enhance its performance.

MAJA MILOSAVLJEVIC, CIA, CRMA, *is an internal auditor at Borealis AG in Vienna, Austria.*

Fraud Findings

BY BRYANT RICHARDS

THE OPPORTUNISTIC CFO

When a small, growing company hires an internal auditor, it discovers the chief financial officer embezzling profits.

In 2009, LeBarge Inc., an oil rig company, was growing beyond the size of a typical small business. The owner and CEO, Lou Smith, decided to hire an accounting firm, which recommended that he add an internal auditor to the team to ensure his control environment kept up with the expanding needs of the business. Concerned about the cost of hiring a full-time person with salary and benefits, Smith decided to forgo the recommendation.

Each year for the next five years, the accounting firm again recommended that Smith hire an internal auditor. LeBarge continued to grow, but profits were shrinking. Smith could not understand why. Costs should be going up, but they were growing faster than revenues. The company's chief financial officer (CFO) and Smith's longtime friend, Jennifer Hagan, offered reports showing increased vendor costs and evidence of inflation. None of this made sense to Smith, as his intuition suggested profits should be up $200,000 annually. In 2014, Smith reluctantly agreed to hire veteran internal auditor Corey Ortiz.

Ortiz joined the company and quickly scoped out his first review of the highest risk area, the financial ledger, which was in QuickBooks. Ortiz prepared a standard audit program that focused on journal entry and reconciliation controls, system access rights, and segregation of duties. The program included walkthroughs of journal entries to evidence support and authority for the recording processes. Bank reconciliation testing was included to understand the process and follow transactions from the ledger to the reconciliation. The program included pulling and reviewing samples of journal entries and reconciliations to check for completeness, timeliness, support, and authorization. And finally, the plan included getting administrative access to QuickBooks through IT and viewing roles and rights within the system.

Ortiz wanted to get off to a strong start and help the organization understand the internal audit process. He spent two weeks creating an audit program, scoping memos and other official communications. He communicated with his stakeholders in polite and professional emails, requesting samples and employee interviews.

The fieldwork began on the first day of week three. Samples were pulled and Ortiz started with the IT manager, who was prepared to show him around the QuickBooks program. At 11:00 a.m., Ortiz stopped the audit and contacted the CEO for an immediate meeting.

Ortiz explained to Smith that while reviewing

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

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

LESSONS LEARNED

- » Companies that expand, whether large or small, are exposed to new risks. Controls designed for the business often stretch and break. In small companies, daily supervision and involvement by the owners often provides significant control value. Decreased supervision in a growing business causes normal control weaknesses, such as segregation of duties, to become glaring opportunities for waste or abuse.
- » Owners of small companies are not risk professionals. Growing companies are rarely prepared to identify and mitigate the expensive risks associated with their new success. Internal auditors are trained risk professionals and provide organizations with resources focused on identifying, preventing, and managing these risks.
- » Start with the ledger and work outward. Access controls and segregation of duties within the financial systems are the cause of many frauds. Trusting one person to manage the financial resources of any company is a dangerous strategy and should always be top of mind for any internal auditor and the first place to look.
- » Know the financial system's logging and reporting features, as small systems sometimes don't have robust controls. Reviewing reports on various changes, such as mailing addresses, employee name, and vendor name, can lead to early fraud detection.

the system administrative rights in QuickBooks, he found that the CFO, Hagan, was the only person with access to the system. This meant that she could create entries, make payments, and edit all data within the system with no checks and balances. It was not surprising to Ortiz that a small company with recent growth had such glaring segregation of duties issues within its ledger. However, a quick review of the system audit logs for the previous month showed numerous changes to payment fields, which is unusual in the normal course of business. He then checked the names of the vendors before they were changed in QuickBooks.

After the meeting with Smith, Ortiz spent the rest of the day working with the IT manager to identify vendor name changes that occurred over the past year. The next morning, Ortiz and Smith called a meeting with Hagan. Ortiz asked her to explain each vendor name change. Hagan was clearly uncomfortable, but offered an excuse about how the system has errors that need to be fixed sometimes.

Skeptical about the explanation, Ortiz started the next day by requesting a vendor spending report for the previous year. He then contacted each vendor and asked them to provide an updated billing summary for that time period. When Ortiz compared the reports, he found a $250,000 discrepancy for the past 12 months.

By the end of the day, Ortiz, Smith, and the human resources manager confronted Hagan with this information. For 15 minutes, she acted surprised and hurt at the accusation. Smith suspended Hagan without pay while the investigation continued. Law enforcement was notified the next day.

In 2017, Hagan was tried and convicted of embezzling more than $800,000. For five years, she used the company's financial ledger as her personal checkbook to pay bills and purchase items. She would later change the vendor name in the payment information fields to a business-related vendor. By slowly increasing her theft as the business grew, she was able to convince management that the expenses were related to challenges associated with normal business growth.

Hagan pleaded guilty to a felony charge of aggregated theft. Before her plea agreement, she paid back half of the money she stole and agreed to pay the rest when her six-month jail sentence concluded. LeBarge has recovered its status of profitability. Ia

> **She used the company's financial ledger as her personal checkbook to pay bills and purchase items.**

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

The Right Path

With help from internal auditors, organizations can reap the performance benefits of ethical decision-making.

Russell A. Jackson

Illustration by Sean Yates
Base photograph by Konstanttin/Shutterstock.com

There are vivid examples of the link between organizations' ethical behavior and their bottom lines. At press time, Kraft Heinz Co. announced restated earnings involving irregularities in its accounting procedures and internal controls; the initial report of the U.S. Securities and Exchange Commission's (SEC's) related subpoena contributed to an almost 20% single-day drop in the company's stock price. Similarly, cryptocurrency company Longfin's shares plunged 30% when it disclosed an SEC investigation last year. And following the news of Volkswagen's now infamous emissions scandal, its stock, too, experienced a 30% decline.

As evidence mounts that ethical business behavior leads to better business performance—boosting stock price performance by almost 15%, according to one estimate—internal auditors need to sharpen their people skills, listen better, and share what they learn with more moving parts in their

organizations' ethics infrastructures. And they need to step up, state their case, and start getting the credit they deserve for doing so.

Stakeholders may understand that internal audit plays a role in ethics, though they may not fully appreciate the breadth of contributions practitioners can make. Now internal auditors have numbers to show how much value the function actually adds.

> "If there's an ethical issue in an area, you can bet there's going to be a business concern—fraud, noncompliance, or weak controls—too."
>
> Karen Brady

> "All aspects of an ethics infrastructure are important, but culture contributes the most to business performance."
>
> Jane Keller-Allen

REPUTATION AND CULTURE

The Ethisphere Institute, a global ethics rating and advocacy firm, names its World's Most Ethical Companies each year, based on the quality of their ethics and compliance programs, organizational culture, corporate citizenship and responsibility, governance and leadership, and reputation. Ethisphere's belief that "financial performance and ethics go hand-in-hand" is validated, it says, by its "Ethics Premium." The organization tracks the stock prices of its publicly traded honorees and compares them to a large cap index—and it says those companies outperformed the index by 14% over five years and by nearly 11% over three years.

Is the connection really cause–effect? Does ethical behavior lead directly to better business performance? "I firmly believe it does," says Karen Brady, corporate vice president of audit and chief compliance officer at Baptist Health South Florida, in Coral Gables—a nine-time Ethisphere honoree. She notes that Ethisphere's reputation criterion is based in part on a Google search of the organization, adding: "Having a good reputation will get you better business. That's a pretty-well-known fact." Ethisphere also cites studies showing that millennials want to do business with companies that have solid ethical reputations, and its CEO Timothy Erblich adds that "employees, consumers, and stakeholders value companies that show a commitment to business integrity."

Of the elements Ethisphere says undergird an entity's ethical behavior, the one that contributes most to business performance is culture, Brady says. "It has to be," she stresses. "The whole thing starts with culture. If you don't have that tone at the top, the organization isn't going to be committed to good governance or good citizenship." Indeed, organizations with a culture that encourages concealment of compliance or other issues, she says, risk severe damage to their reputations.

Jane Keller-Allen, vice president of Internal Audit, Compliance, and Risk at WPS Health Solutions in Madison, Wisc., also stresses culture's influence on the bottom line, and she agrees that tone at the top is key. "All aspects of an ethics infrastructure are important, but culture contributes the most to business performance," she says. "The culture of an organization is usually driven by its leaders. If leadership believes in doing things the right way, then compliance programs and corporate citizenship will naturally flourish under that direction."

Keller-Allen adds that if the organization's leaders help establish a culture that fosters trust, then employees will be more inclined to report potential compliance issues. And that, in turn, enables the organization to resolve any issues more quickly.

At Baptist Health South Florida, internal audit contributes to ensuring that ethical behavior begets profits in several ways. "From time to time, we audit each of the Ethisphere criteria," Brady says; that includes informal surveys in the departments and locations they audit. And, she says, "ethics is huge when we assess risks," citing trends in hotline calls and human resources (HR) statistics as potential red flags. She adds: "If there's an ethical issue in an area, you

16% of employees experienced pressure to compromise ethical standards, a 23% increase since 2013, according to the Ethics & Compliance Initiative's 2018 Global Business Ethics Survey.

ETHICS TECH

Technology that enables compliance and ethics-related information-sharing, including input from internal audit, is becoming increasingly sophisticated, says OCEG President Carole Switzer – and the best may be yet to come. "Technology that incorporates internal audit findings that flag issues – and that sets a process for notifying relevant parties so that they can address deficiencies and respond to the concerns raised – is hugely helpful," she says. The opportunity for business operations to input their information into the same system as risk, internal audit, and human resources is, she adds, "a bit of a game changer."

Recent technological advances have enabled central hubs that pull in data from multiple systems inside and outside an organization and make it available across the enterprise, she explains. "That combined with advanced machine learning, other types of artificial intelligence, natural language processing, and predictive analytics," she says, "represents the real revolution."

The revolution "benefits internal audit's ability to really dig in and understand what's being done to address risk on a completely different level," Switzer adds. "Internal audit can help other stakeholders use those capabilities to create a living, strategic planning process."

can bet there's going to be a business concern — fraud, noncompliance, or weak controls — too."

Jeff Dougher, internal audit director at Intel in Portland, Ore., agrees that the profession has an important role in effective assessment of business performance as it relates to ethics — by virtue of being an independent advisor. "That could be as simple as spending time with first-level managers and staff to see how they would raise issues, and teaching individuals how and where to report issues," he says. Internal audit can help management understand the types of messages business managers proliferate throughout an organization, he adds, and can help "ensure the culture of ethics and compliance is consistently understood throughout each particular group or team." Intel has been recognized on the Ethisphere list seven times.

TEAMWORK AND PARTNERSHIPS

In fact, internal audit has all kinds of ways to help drive and assess a company's ethical behavior, Dougher says. Being independent and keeping individuals' interviews anonymous allows internal audit to "ask clarifying questions that provide accurate information and valuable insight to help management understand their site cultures," he adds. Teamwork matters, too. "We partner with the Ethics and Legal Compliance (ELC) program for selected audits," Dougher explains, "helping ensure management has established appropriate ELC programs throughout their business groups and site programs."

Gerry Zack, CEO at the Society of Corporate Compliance & Ethics and the Health Care Compliance Association in Minneapolis, recognizes the value of such practices. He says high performing organizations "have partnerships between compliance and internal audit and between internal audit and other entities in the enterprise that directly affect culture and ethics." HR is one of them; so is senior management. Zack says this is often part of internal audit's advisory role.

Carole Switzer, co-founder and president of OCEG (formerly the Open Compliance & Ethics Group) in Phoenix, also cites the value of cross-functional partnerships. She suggests

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

rotating internal auditors through roles in risk management and compliance to afford them a bigger picture perspective on an integrated governance, risk, and compliance process structure. "The key thing to recognize is any of the moving parts of the 'ethics infrastructure' can be the cause of failure," she says. "You cannot establish strong culture, for example, if you don't have strong leadership with clear vision and commitment."

The key to taking a company's ethical temperature is finding out what its stakeholders think. Ethisphere says its World's Most Ethical Companies "cultivate a culture of integrity"—by measuring employees' comfort with speaking up, for example, and their views of leadership's trustworthiness, and by "leveraging a broad array of tools and techniques to get a sense of their internal ethical cultures."

Some companies use a dedicated ethics survey process, Ethisphere says, adding that "pulse-type surveys to capture small, but frequent, readings of ethical temperatures across the organization are oft-discussed, but rarely used." Employee engagement surveys are the most popular ethical thermometers, Ethisphere reports; the percentage using them rose 12 points from 2017 to 2018. Ethisphere adds that such surveys are driven primarily by the HR function, with regular frequency and broad distribution.

"Whether it is asking a site-specific question or evaluating a particular area, we want to ensure all parties are aligned ahead of time."

Jeff Dougher

AUDITING BY WALKING AROUND

Surveys themselves won't provide all the information internal audit needs. In fact, using annual queries in isolation to get a feel for ethical culture is not very useful, Switzer says. "If you have a huge problem, you may find it, but you won't find the more subtle or complicated things."

That more nuanced insight requires what Zack calls "the walking around approach, talking with people." He adds: "The casual conversation that begins with, 'How are things going?' can lead to amazing insights if you let it."

That's true for small companies, too, Brady points out. "For internal audit to have a sense of the organization's culture, you have to do site visits," she says, "even if that's a 'department' visit."

And that's what Ethisphere's World's Most Ethical Companies are doing; the percentage of those companies conducting site visits jumped 28 points from 2016 to 2018, reflecting what the organization calls "a growing relationship between the compliance function and other control functions, like internal audit, that are regularly in the field." Indeed, the report that accompanies the Ethisphere listing notes that "more companies arm internal audit with questions to ask during site visits, collaborating more closely with HR and safety."

As part of Intel's annual plan, Dougher's team evaluates international site coverage to ensure it has the right balance of audits. "The audit program evaluates specific risk indicators—including factors such as growth, location, and spending—to understand any changes to the site to better understand if an audit should be performed," Dougher says. The site audit program includes interviews with all levels, he adds, "to help understand how ethics is interpreted and help management understand the site's culture." His team also has used site-level surveys—working with HR and legal on wording—to reinforce messaging, as well as open forums and workshops.

ON THE SAME PAGE

To help standardize information, Dougher says he partners with Intel's ELC program to ensure all parties are aware of each other's coverage. "Whether it is asking a site-specific question or evaluating a particular area, we want to ensure all parties are

Only 38% of ethics, compliance, and legal professionals say senior leaders at their firms support disciplinary action against high performers guilty of misconduct, according to a 2019 LRN Corp. survey.

aligned ahead of time," he explains. To that end, Dougher says Intel has developed a standard test program and a standard set of questions internal auditors use to identify trends and talk about key points with management. The critical factor from his perspective is "ensuring the template is being used across each audit program and documented within our audit methodology."

Brady adds: "We all are interdependent." Part of risk assessment is looking at trends, she explains; internal auditors evaluate hotline data they receive from compliance and may ask why they keep hearing about conflicts of interest, or about a particular compliance issue. "Internal audit needs to make sure the issues are escalated," she comments, "and thoroughly investigated when necessary."

Moreover, trends in turnover statistics may prompt a conversation about a department—or an audit may reveal a potential HR concern—and the same applies to quality improvement. "We give feedback to HR, compliance, quality, and other functions when we identify trends or issues that affect them," Brady says. "That happens routinely."

Sometimes the ethics-related feedback is especially sensitive. A casual interview in an audit may turn up comments about, for example, sexual harassment, raising the question of how to appropriately use casual comments, body language, and other signals as data for assessing a situation and recommending responses.

"It comes down to people skills," Brady states. "We do our best to train auditors that when they hear something like that in an interview they should ask the next question: 'What do you mean by that?'" If that individual doesn't reveal anything else, she suggests asking others in the department if they have any concerns. "It's the best you can do," she says. "Ninety-five percent of the time, it's successful."

Zack adds: "Talking to people is an auditing and monitoring step that can be institutionalized. But there's also a certain percentage of using the information that's seat of the pants, what your gut tells you."

MAKE THE CONNECTION

Too often, what the gut says is, "mind your own business," Brady says. "I hear from a lot of internal auditors who say they'd never start a conversation about culture or diversity or corporate responsibility with their stakeholders because that's not their stakeholders' expectation of internal audit." Too many internal audit functions, she adds, remain "focused on 'check the box' compliance or financial audits, and don't realize that the important thing is to make sure their stakeholders are aware of *all* risks—not just the traditional ones."

Stakeholder underestimation needs to change, and the profession needs to change it. "It could be a good approach to link elements of audited programs to strategic objectives of the organization, including business performance," Zack suggests. When the compliance program is audited, for example, each underlying activity—training in a particular area, for example—could be sized up in part by asking, "How does that help the business? How does it contribute to the performance of the organization?"

Those links then need to be promoted. "We absolutely should talk about it more," Brady emphasizes, pointing again to the connection between business ethics and performance. "Stakeholders need to understand how important that is and, as chief audit executives, we need to make sure they understand that internal audit has a much broader perspective," she says. "We need to do more to get that point across." Ia

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

"The key thing to recognize is any of the moving parts of the 'ethics infrastructure' can be the cause of failure."

Carole Switzer

"The casual conversation that begins with, 'How are things going?' can lead to amazing insights if you let it."

Gerry Zack

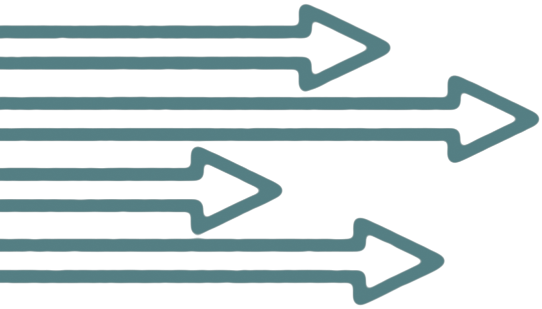
IN LINE WIT

Implementing a risk management program can better align an organization's risk profile with its overall strategy.

Dorina Hamzo

H RISK

Risk management has evolved and grown since its inception in the mid-20th century, as evidenced by the introduction of methodologies such as The Committee of Sponsoring Organizations of the Treadway Commission's (COSO's) *Enterprise Risk Management–Integrating With Strategy and Performance*, the International Organization for Standardization's ISO 31000, and the Basel Accords. Yet, only 23% of respondents describe their risk management program as mature in the American Institute of Certified Professional Accountants' 2019 The State of Risk Oversight, conducted jointly with North Carolina State's ERM Initiative. Additionally, the perceived level of maturity has declined over the past two years, and most organizations struggle to integrate their enterprise risk management (ERM) program with the strategy and objective-setting process.



TURGAYGUNDOGDU / SHUTTERSTOCK.COM

Understanding and managing risk has tremendous benefits, as it helps organizations better prepare for the future. So why aren't ERM programs more mature and better accepted? Most likely it is because organizations do not know how to develop a program or because they do not embrace risk management.

The current way of thinking about this practice can be challenged to discover new ways of evolving it to more effectively manage strategic risk. My former organization developed and successfully implemented an ERM function, and I am currently using the same strategic program to build a function at Covetrus, an animal-health technology and services company. Building a systematic and strategic program at my former company was educational and rewarding, as it allowed my team and me to familiarize ourselves with many aspects of the organization.

WHERE TO BEGIN

Before establishing the program, my team and I identified key points of concern that needed to be addressed during implementation:

» Risks were too generic to create measurable plans.

» Issues and controls were not systematically mapped to risks.

- It was difficult to quantify and qualify the impact to the organization.
- Progress tracking of risk remediation plans was not well-documented.

The program implementation was then divided into three phases spanning several years.

PHASE 1: PILOT

During this phase, the team developed a detailed risk library and hierarchy that aligned with the organization's life cycle, mapped issues and controls to risks providing a real-time picture of the organization's risk profile, developed measurable remediation plans for the top risks, and implemented centralized reporting.

Participation in the risk program initially was limited to the internal audit, vendor due diligence, and compliance teams. Some of the key steps taken to complete this phase included:

- Selecting an ERM standard. We decided on COSO's updated ERM framework.
- Defining purpose, scope, roles, and responsibilities.
- Formalizing a risk-rating methodology.
- Developing a master risk library.
- Documenting a process for identifying risks, assessing severity, implementing responses, tracking, and reporting.
- Conducting initial risk assessments with critical areas.

The development of the risk library was vital, as it defined the program foundation and provided common terminology for all of the program participants. Over time, the team updated the library based on management feedback to customize it to the type of risks inherent to the organization. The team organized risks into a three-tiered hierarchy. At the top were the key enterprise risk areas, which follow the organization's life cycle (see "Enterprise Risk Areas" on page 33).

Underneath each enterprise risk area, there are intermediate risks that represent the subfunctions of that risk area. Within each intermediate risk, there are individual risks that are potential events that can impact that business area. The individual risks are linked to processes, objectives, key risk indicators, financial losses, mitigating controls, incidents, and findings (see "Risks, Controls, Issues, and Remediation Mapping" on page 35).

Mapping the more than 900 internal controls and issues to each individual risk took the most time, but it was the most important step. Mapping processes provided further insight into the ratings, which often are subjective. More specifically, the occurrence of an issue increased the likelihood, while the presence of compliant internal controls decreased the likelihood, of one or more risks occurring.

After the completion of this phase, we realized that we tried to accomplish too much in too short a time. For example, we defined the end-to-end risk process while simultaneously automating it via our risk management system. Looking back, we should have operationalized the process before introducing a tool.

PHASE 2: IMPLEMENT THE PROGRAM

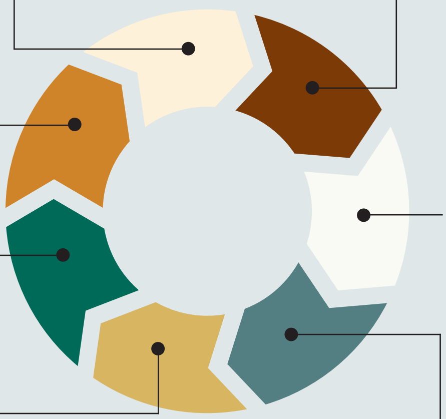
During phase 2, my team and I developed a formal risk management policy, fine-tuned the process, expanded risk assessments across all divisions, and established a governance committee. The team also incorporated other key risk management functions under the umbrella of the ERM program to include business continuity, information security, legal, and patient safety teams.

The individual teams had their own governance committees, which were consolidated into a single

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

83% of financial organizations have an ERM program in place, up from 73% in 2017, according to Deloitte's 2019 Global Risk Management Survey.

ENTERPRISE RISK AREAS



Governance
- » Corporate Governance
- » Ethics

Strategy & Planning
- » Corporate Responsibility & Sustainability
- » External Factors
- » Planning
- » Strategy
- » Mergers/Acquisitions/Divestitures

Reporting

Compliance

Infrastructure
- » Corporate Assets
- » Finance
- » Human Resources
- » IT
- » Legal

Operations
- » Intellectual Property Management
- » Product Life Cycle Management
- » System Development Life Cycle Management
- » Outsourcing
- » Offshoring
- » Supply Chain
- » Customer Contract Management
- » Customer Support

Innovation & Growth
- » Innovation, Research, and Development
- » Product Development
- » Sales, Marketing, and Communications

governance, risk, and compliance team comprising executive leadership. This team met several times a year to discuss top risks and the status of remediation plans, and to escalate critical issues, as necessary.

Issue tracking from these key functions was consolidated into one consistent process and tool. This effort took one year, and we followed the same process for each team:

- » Conduct current state analysis of processes, people, and tools.
- » Normalize rating methodologies.
- » Migrate all open issues and implement a process for identifying and tracking issues and remediation plans in the ERM system.

To ensure accurate risk tagging for these issues, we configured the tool to route any new issues to the risk management team for approval. We used the review as a learning opportunity for both our team and the business where once a month we reviewed issues, related root causes, remediation plans, and impacted risks.

PHASE 3: INTEGRATE ERM WITH THE STRATEGY

Early in our process, we learned that a successful integration is dependent on the organization having a strategic approach for identifying, managing, and reporting on the strategy and objectives. Integration with the ERM program becomes just one of the steps in that process.

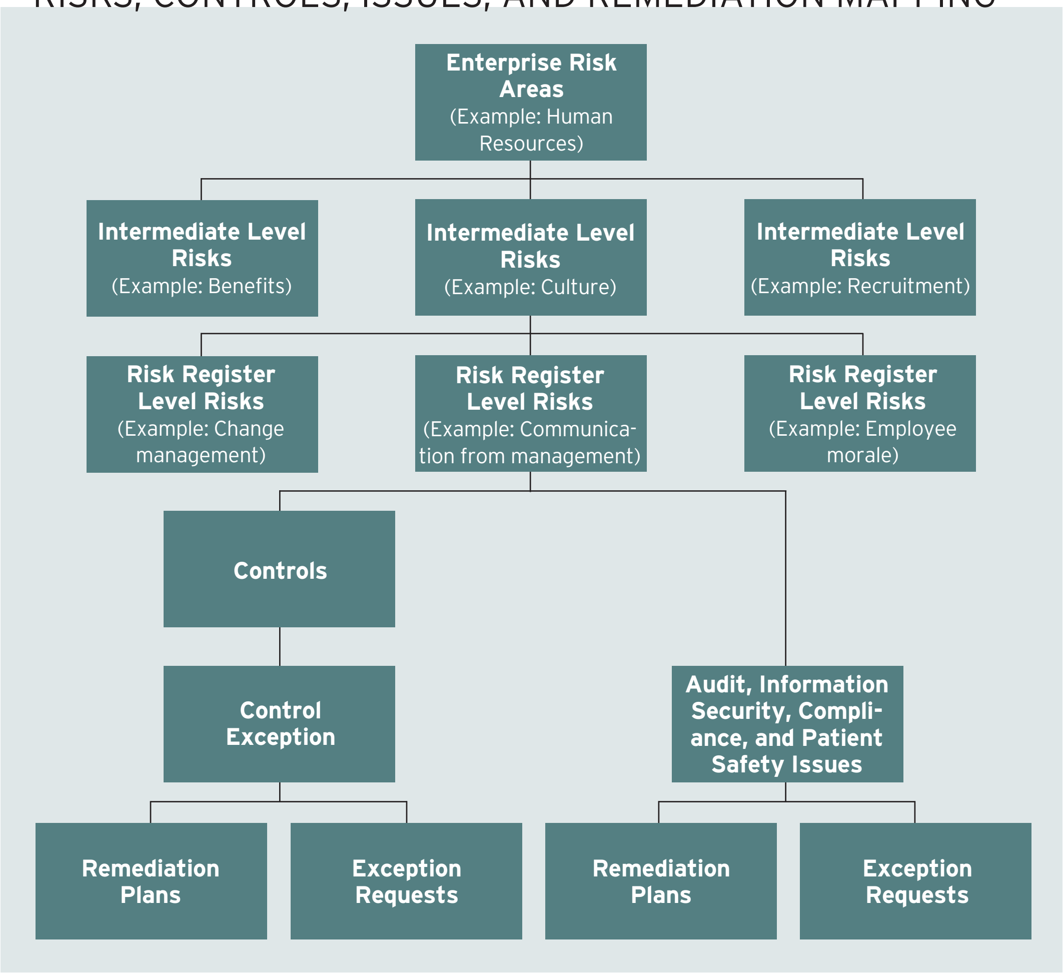
The integration process started with the definition of our risk appetite statements for each of the company objectives. For example:

- » Objective: Develop new products and attract new customers.
- » Risk Appetite: An organization will not make decisions that compromise its reputation by using defective new products that introduce security vulnerabilities and cause customer data breach.

Next, the leadership team identified projects or initiatives that supported the organization's objectives and strategy and included information such as opportunities, dependencies, resources, budget, and timeline. Coordination with the general and administration functions to discuss resource and budget needs, as well as

Collaborating and aligning to provide a consolidated view of risks is a habit of risk functions that fuel smarter risk taking, says PwC's 2019 Risk in Review study.

RISKS, CONTROLS, ISSUES, AND REMEDIATION MAPPING


Enterprise Risk Areas (Example: Human Resources)
Intermediate Level Risks (Example: Benefits)
Intermediate Level Risks (Example: Culture)
Intermediate Level Risks (Example: Recruitment)
Risk Register Level Risks (Example: Change management)
Risk Register Level Risks (Example: Communication from management)
Risk Register Level Risks (Example: Employee morale)
Controls
Control Exception
Audit, Information Security, Compliance, and Patient Safety Issues
Remediation Plans
Exception Requests
Remediation Plans
Exception Requests

any regulatory and compliance implications as a result of these projects, was necessary, as these dependencies could become risks to the objectives. This included human resources, legal, audit, and finance planning and forecasting teams.

The ERM team, partnering with leaders, identified additional risks at the project level. These risks were rated using the rating methodology and rolled up to the enterprise level. The prioritization and responses to the risks were aligned to the risk appetite statements. These statements also will guide the organization's response to emerging risks that surface throughout the year.

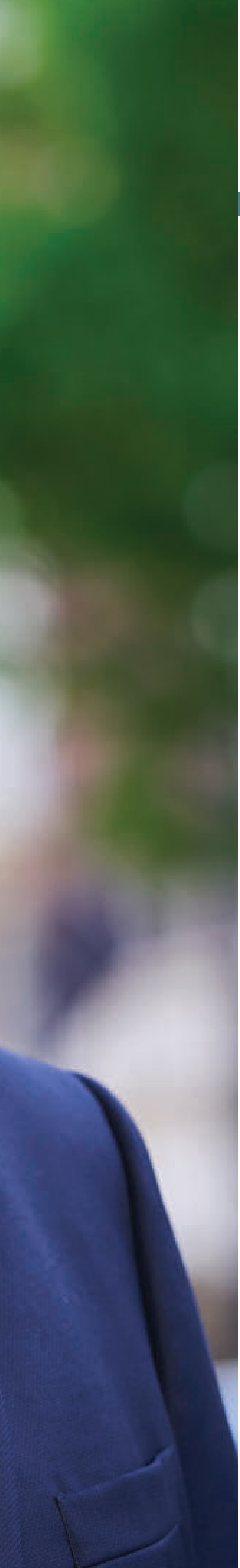
ORGANIZATIONAL ALIGNMENT

Throughout this program, the team learned to work more productively with the organization in order to be met with less resistance. From the start, we learned that discussions about risk without the right approach can be perceived as an attack and critical of the business.

As a result of this project, the team embraced a teaching and learning approach where we spend more time educating the organization about risk principles, which helped us better understand business and risks from the organization's perspective. Collectively, the organization became more aligned with its risk profile.

Internal auditors can make a difference if organizations overcome their giving-up point. By giving risk management a try and not waiting for a big event to happen that forces internal auditors to adopt risk management haphazardly, they are doing right by their organizations. Progress cannot be made through fear.

DORINA HAMZO, CISO, *is vice president of internal audit at Covetrus in Portland, Maine.*



Step *forward*

IIA's 2019-2020 North American Board chair, BENITO YBARRA, says internal auditors can do more to enhance and protect organizational value.

Throughout my 20 years as a student and practitioner of internal auditing, I have seen the profession make strides toward achieving its full potential. However, there is still more to do. If the full scope of internal audit's work today is seen as ensuring the accuracy and reliability of information, opportunities to make a bigger difference and reach our potential are being squandered. Contemporary internal auditors must contribute to advancing the strategies and business practices of their organizations. Today's internal auditors also must be an example of integrity and a force that drives the kind of good, sound culture that is the foundation of successful enterprises (see "The Right Path" on page 24). In short, to operate at the highest levels of the business, internal audit must "Step Forward"—my theme

Photographs by Darren Carroll

for my year as chair of The IIA's North American Board.

Three areas of opportunity for internal auditors to step forward fall under the headings of culture, courage, and conflict. There are still those practitioners who do not fully understand what the role of an internal auditor entails—or, if they do, they are unwilling or unable to take the necessary steps toward fulfilling that role. First, setting the right tone by conducting oneself with professionalism and competence is key—own the role unapologetically and without reservations. Second, some internal auditors lack the courage to make disruptive and strategic recommendations for improvement to management and the board. And, finally, some auditors are simply uncomfortable with conflict. They fail to understand that embracing conflict can help them produce better, more robust work.

I urge internal auditors who struggle in these areas at any level of the profession and in any type of organization to *step forward* and begin making a bigger difference for themselves, those they serve, and the profession.

CULTURE: DO WHAT'S RIGHT

It is part of internal audit's job to help drive a prevailing culture within the organization that is fair, healthy, effective, and focused on serving customers—an organization that one can trust. Securing a position of trust is not easy. When I accepted my current role as chief audit and compliance officer at the Texas Department for Transportation (TxDOT) in 2011, I was called on to improve the profile of the audit department and the organization. Immediately, my defense mechanism kicked in: Yes, I was responsible for how the audit department was perceived; no, I couldn't own responsibility for the organization's profile. In the end, I took on the challenge and, in partnership with my commission (board), initiated a program to elevate the focus on holding ourselves accountable, being transparent, and examining how and with whom the organization conducted its work.

One of the first steps, an external audit, identified noncompliance as well as some impropriety at an entity that did business with TxDOT. It would have been easy to call out the noncompliance, issue a report with recommendations, and be done with it. However, it was an opportunity to demonstrate that TxDOT was serious about its stewardship role. I positioned this to my audit committee chair as a chance for the organization to demonstrate that it was focused on driving honesty, integrity, and trust in its business relationships. Internal audit aligned with the board and executive leadership in formulating a strategy to anticipate and get ahead of any pushback from the entity's officials. In addition to meeting with the entity's leaders, I met with local officials and equipped TxDOT's board and executives with information to share with our state officials. It was uncharted territory, but we knew it was the right thing to do, and we did it. It was the beginning of improving the profile of the audit department and the organization.

It was uncharted territory, but we knew it was the right thing to do, and we did it.

To set course on such initiatives, internal auditors must be able to work strategically and operationally at all levels of the organization. That entails evaluating the business to understand how it could do things differently to better serve customers—how it can achieve goals at the same time as building trust and a more sustainable culture. Recommendations must be relevant and practical. Internal audit's oversight role puts it in a unique position to help the business in these ways.

Chief audit executives (CAEs) must engage their boards and advocate for internal audit by explaining its value to the organization. It is not always understood, for example, that internal audit is here to make things better. Even where

FROM THEN TO NOW

After graduating from the University of Texas in 1993, I expected to pursue a career in law. Instead, I decided to take a break from school and accepted a job collecting student loan payments at the Texas Guaranteed Student Loan Corp. I worked my way up to investigator and, eventually, to internal auditor. The investigator job reported to the internal auditor, who allowed me to work on an audit. I really loved that, especially interviewing people and learning about things that were considered confidential. It was so interesting to me being in that environment.

In 2006, I joined the technology solutions business Dell Inc., which had been focusing on improving its culture by "Winning With Integrity." Dell was using the internal audit department to drive change across the business. I was assigned to assist with the organization's first external quality assessment, including working on its first internal audit charter. It was a great learning experience to understand how a Fortune 50 company could rally around an internal audit initiative. Dell really did implement a world-class audit function, and I learned so much from that organization. I'd be remiss if I didn't mention Mike DeCaro, vice president of Corporate Audit at the time, who challenged me and everyone to be more than technically adequate, and to step forward and strive for excellence.

Joining the Texas Department of Transportation (TxDOT) in 2011 was an opportunity for me to help modernize an audit department and help it drive change in the business. Today, I oversee TxDOT's internal audit and compliance divisions, which are aimed at improving stewardship, risk management, accountability, and governance through value-driven audits, evaluations, investigations, and advisory services engagements.

During my more than 20-year career, I have served in various positions with the IIA–Austin Chapter, including as the 2006 president. I have been a member of The IIA's Professional Issues Committee, Publications Advisory Committee, and Public Sector Advisory Committee. I've served as vice chair of both content and professional development and as senior vice chair on the North American Board. Now, as chair of the North American Board, I also have a seat on The IIA's Global Board. I am a member of the American Center for Government Auditing, American Association of State Highway and Transportation Officials, and several other professional organizations. I am past chair of the Texas State Agency Internal Audit Forum. I have earned the Certified Internal Auditor, Certified Information Systems Auditor, Certified Fraud Examiner, and Certified Compliance and Ethics Professional designations.

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

LEFT: WILLIAM VAN OVERBEEK; RIGHT: DARREN CARROLL a good relationship exists, there may be opportunities to extend internal audit's reach. For example, recently numerous accounts of harassment in the workplace have been brought to light. Few would instinctively think of internal audit as ideally positioned to help address such an important, culturally explosive issue. Instead, they would reach out to human resources or the legal department. But internal audit can act as the eyes and ears of the board on such sensitive issues and help gauge the culture in different parts of the enterprise. Every audit opens the door to understanding how business is conducted, but it also is an opportunity to understand the culture of those performing the work. Internal audit needs to step forward and ask questions to ensure it feels good about the organization's health.

IT TAKES COURAGE

During my career, I've conducted many external quality assessments. Invariably, I request time with each member of the board to understand his or her knowledge of the CAE's role. Their feedback often includes: CAEs do not communicate effectively; CAEs do not focus on matters that are important enough to rise to the board level; and the time CAEs have with the audit committee and their reporting executive manager is insufficient. These are indications CAEs are not stepping forward to make their value known, and their work is not perceived to be informing or advancing the success of the organization. Perhaps they do not understand their organizations as well as they should, or they are not fully engaged with how their organization's leadership plans aim to achieve its strategic goals—issues that come up time and again in IIA research and surveys.

The North American Board has asked The IIA to focus on advocating for the internal audit/board relationship through the creation of tools and content that will help CAEs have the courage to step forward. In the meantime, CAEs can take it upon themselves to get to know individual board members and executives. CAEs need to understand the priorities of the entire board, not just the audit committee. It takes courage to ask for time with the board, but the context and perspective obtained from those conversations help make internal audit's work meaningful.

More junior staff can step forward by spending constructive time with senior auditors. It can take courage to speak to CAEs for those just beginning their careers, but it will be worth the effort. Junior staff also should get involved with their professional organizations—The IIA has many local chapters and special interest groups. If these auditors are only learning from their companies, they are missing out on great ideas they can bring back to their teams.

EMBRACE CONFLICT

While it may sound counterintuitive, internal auditors should treat every

MY YEAR AS CHAIR

During my year as IIA North American Board chair, my focus will be encouraging a renewed emphasis on helping internal auditors realize and appreciate that they are part of an indispensable profession. That entails providing IIA members with the tools they need to step forward in their organizations—to help them balance their often deep technical proficiency with the ability to instill confidence in their stakeholders that internal audit can make a difference at a strategic level and provide leadership.

In addition, in North America and globally, The IIA is striving to achieve concrete results from its advocacy work. We have been advocating, for example, for the U.S. Securities and Exchange Commission to require publicly traded companies to disclose whether they have an internal audit function. This is the first of many steps required to provide The IIA with the impetus to go further and begin a public discussion about what it means to be a professional internal auditor who follows the *International Standards for the Professional Practice of Internal Auditing* and the criticality of holding a Certified Internal Auditor designation.

I am also chairing an IIA group that is reviewing the committees of the North American Board to ensure our professional body is streamlined and fit-for-purpose. We are assessing whether each committee is still adding the value that we initially envisaged. The review most likely will lead to restructuring, change, and spirited discussions. When people are passionate about what they do, it is crucial that those involved can see the bigger picture and bring their considerable skills and talents to bear on the most relevant and strategic issues. So, we are looking at the North American committees as well as the relationships between that body and global committees under the One IIA initiative, which is aimed at achieving better uniformity of internal audit quality globally.

I want auditors to understand that internal auditing is a noble and indispensable profession.

engagement as an opportunity to deal with potential conflict. At TxDOT, for example, we deliberately include conflict in our audit processes and find it to be a powerful tool. For instance, when our audit teams explain their recommendations regarding an audit's scope of work, or what testing they are planning, the internal audit management team is charged with challenging it. That puts the teams through a level of conflict that helps them support the work they want to do and the reasons they want to do it; and it can identify gaps and weaknesses to help make the audit work stronger. It also pushes the management team to put itself in the business owners' shoes, which requires deep knowledge of the business and its leaders to be effective. My role is to challenge the management team by bringing a board and executive management perspective to the forefront. I ensure that the message we are delivering will matter, and that we account for potential organizational and political considerations.

We have such meetings at the planning, fieldwork, and reporting phases of each audit. This process prepares staff members to sell their ideas and value to our business partners—it helps everyone in the organization. It can be tough going through this process, but we remind our team that it is a safe environment, and it is orchestrated to help them deal with the conflict they will sometimes face out in the field. It would be a disservice to my team not to do so.

ENHANCING VALUE

I accept that a year is not a long time to effect all of the changes mentioned herein. At a minimum, I would like to hear more stories about internal auditors stepping forward and adding value to their organizations. I want to continue to push for a shift in the way publicly traded companies view and talk about the profession. But, most of all, I want auditors to understand that internal auditing is a noble and indispensable profession, and I urge them to have the courage to act accordingly. Ia

BENITO YBARRA, CIA, *is chief audit and compliance officer at the Texas Department of Transportation in Austin.*

Bias in the Machine

Organizations that depend on artificial intelligence models must control for factors that could expose them to discrimination risk.

Allan Sammy

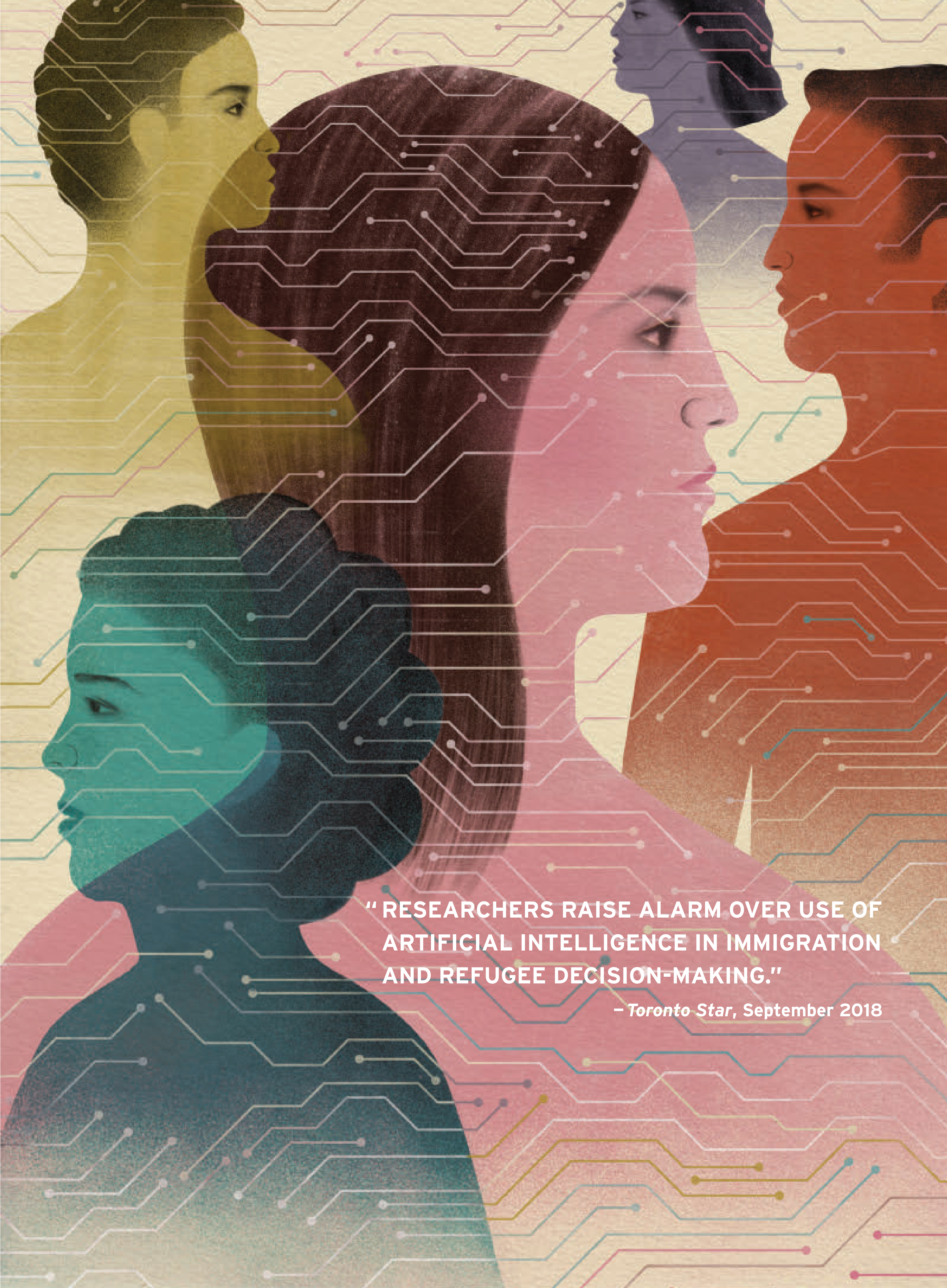
Illustration by Sandra Dionisi

Can artificial intelligence (AI) discriminate? That is what Facebook's AI is accused of doing. In March, the U.S. Department of Housing and Urban Development (HUD) announced it was suing the social media company for violating the Fair Housing Act. HUD alleges that Facebook's advertising system allowed advertisers to limit housing ads based on race, gender, and other characteristics. The agency also claims Facebook's ad system discriminates against users even when advertisers did not choose to do so.

Although it has yet to be proven whether Facebook committed any deliberate discrimination, the result is still the same. "Using a computer to limit a person's housing choices can be just as discriminatory as slamming a door in someone's face," HUD Secretary Ben Carson said in announcing the lawsuit.

Each day, machine learning and AI (ML/AI) models make decisions that affect the lives of millions of people. As these models become more integrated with everyday decision-making, organizations need to be increasingly vigilant of the risk created by potentially discriminatory algorithms.

But who within those organizations is responsible for ensuring the ML/AI model is making fair, unbiased decisions? The model developer should not be responsible, because internal control principles dictate that the persons who create a system cannot be impartial evaluators of that same system. The model's users also should not be responsible, because they typically lack the expertise to evaluate an ML/AI model. Users also may not question a model that



"RESEARCHERS RAISE ALARM OVER USE OF ARTIFICIAL INTELLIGENCE IN IMMIGRATION AND REFUGEE DECISION-MAKING."

– *Toronto Star*, September 2018

MORE VISIT our mobile app + InternalAuditor.org to view a video series on auditing artificial intelligence.

seems to be performing well. For example, if a predictive policing model leads to more arrests and less crime, users are not likely to question whether that system unfairly targets a particular group.

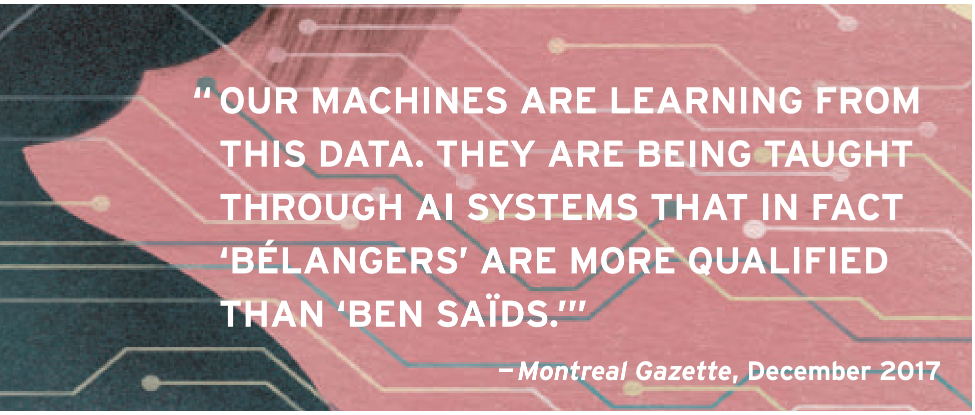
Internal audit may be best suited to provide assurance to the board and senior management that the organization is mitigating the reputational, financial, and legal risks of implementing a biased ML/AI model. However, because this is a new assurance domain for the profession, auditors need a methodology for auditing the fairness of these models.

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

WHY MODELS NEED TO BE FAIR

An ML/AI model is a mathematical equation that uses data to produce a calculation such as a score, ranking, classification, or prediction. It is a specific set of instructions on how to analyze data to deliver a particular result—behavior, decision, action, or cause—to support a business process.

There are three main categories of analytic models. *Descriptive models* summarize large amounts of data into small bits of information that are easier for organizations to analyze and work with. *Predictive models* are more complex models used to identify patterns and correlations in data that can be used to predict future results. *Prescriptive models* enable data analysts to see how a decision today can create multiple future scenarios.



"OUR MACHINES ARE LEARNING FROM THIS DATA. THEY ARE BEING TAUGHT THROUGH AI SYSTEMS THAT IN FACT 'BÉLANGERS' ARE MORE QUALIFIED THAN 'BEN SAÏDS.'"

–*Montreal Gazette*, December 2017

ML/AI models need to be fair and nondiscriminatory because the decisions they support can expose organizations to substantial risk if the classification criteria they use are unethical, illegal, or publicly unacceptable. Such criteria are referred to as inappropriate classification criteria (ICCs) and include race, gender, religion, sexual orientation, and age.

In assurance engagements regarding bias, internal auditors primarily will be concerned with a type of predictive model known as a classification model. This model is used to separate people into groups based on certain attributes that an organization can use to support decisions. Examples of these attributes include:

- » Identifying borrowers who are most likely to default on a loan.
- » Classifying employees as future high performers.
- » Selecting persons who are least likely to commit further crimes if granted probation.
- » Targeting consumers to receive special promotions or opportunities. In one case, the Communications Workers of America sued T-Mobile, Facebook, and a host of other companies, alleging that those companies discriminated by excluding older workers from seeing their job ads.

To provide assurance to management and the audit committee that the organization's ML/AI model does not discriminate, auditors need to assess two things: 1) That the model does not benefit or penalize a certain classification of people; and 2) if a classification is removed from the model, it still provides useful results.

Internal auditors can test for bias using a model fairness review methodology. This methodology comprises:

Automated decision systems could be **regulated** by the U.S. Federal Trade Commission to identify bias and privacy risks under a new Senate bill, the Algorithmic Accountability Act.

CONTROLLING FOR EXOGENOUS VARIABLES

Often, despite the best efforts to eliminate it, discrimination creeps into an organization's analytic models through external data that has a systemic bias, thus exposing the organization to risk. Appropriate exogenous variables (AEV) are variables that provide appropriate classification criteria but have been subject to external systemic bias that has not been detected. An example of AEVs would be the credit score for individuals from minority communities or salary information for women.

Fortunately, analytic models can be used to control for this bias. For example, after controlling for gender differences in industry, occupation, education, age, job tenure, province of residence, marital status, and union status, an 8% wage gap persists between men and women in Canada, according to a February 2018 *Maclean's* article. It is a relatively simple exercise to adjust the salary variable in a classification model by +8% for female subjects.

"SOFTWARE PROGRAMS THAT USE POLICE RECORDS TO PREDICT CRIME HOT SPOTS MAY RESULT IN POLICE UNFAIRLY TARGETING LOW-INCOME AND MINORITY COMMUNITIES, A NEW STUDY SHOWS."

–*Science News*, March 2017

1. Understanding the model's business purpose.
2. Working with the audit client to determine and identify ICCs. In this step, auditors also may discuss possible appropriate exogenous variables (see "Controlling for Exogenous Variables" on this page).
3. Selecting a large sample—or the entire data set—of input data and classification results.
4. Conducting statistical analysis of the results to determine whether distribution of ICCs is within acceptable parameters.
5. Discussing initial results with the client.
6. Removing ICCs and re-running the classification model. Auditors also can replace ICCs with uniform values depending on the nature of the model.
7. Comparing distribution of ICCs before and after removal.

A BIAS AUDIT

As an example of how internal auditors can use this methodology, consider a marketing department at a credit card company that used a classification model to determine which customers should be given a discount. The data used for the model is half women and half men. Management wanted assurance that this model was not exposing the organization to potential liability by discriminating against either group.

Internal audit met with Marketing and confirmed that it used the model to select customers for preferred rates. These preferred rates are substantially lower than the rates offered to customers in general. After reviewing the information used by the model, internal audit noted these variables:

- Customer ID (metadata—not used as a variable).
- Surname (ICC).
- Credit score.
- Geography (ICC).
- Gender (ICC).
- Age (ICC).
- Tenure.
- Balance.
- Number of products.
- Has credit card.
- Estimated salary.

In some cases, a variable may be an ICC for one type of model but not for another. For example, gender is an appropriate classification criterion for a clothing company promotion but not for a loan approval. Age may be appropriate in a health-care model but not in an applicant screening.

In the marketing example, internal audit analyzed the initial results of the classification model and observed that 35% of customers were classified as good candidates. However:

- 50% of men and 20% of women were classified as good candidates.
- 6% of customers over 50 were classified as good candidates.
- 1% of women over 50 were classified as good candidates.

Internal audit discussed the initial classification results with the marketing department to determine whether there are business reasons for the observed result and if those reasons are valid, defensible, and nondiscriminatory to mitigate the risk of legal liability. Based on this discussion, internal audit removed the identified ICC from the input data and re-ran the classification model.

In reporting the results to Marketing, internal audit noted the model was producing useful results. The results showed that 45% of customers were classified as good candidates, a finding with which Marketing concurred. However:

- 50% of men and 40% of women were classified as good candidates.
- 21% of customers over 50 were classified as good candidates.
- 10% of women over 50 were classified as good candidates.

Internal auditors noted that the model appears to be biased against groups such as women and people over 50, which is likely the result of exogenous variables. Auditors recommended that Marketing adjust its model to compensate for these variables.

NEW MODELS, OLD RISKS

Although the subject of bias in analytic models may be unfamiliar to internal auditors, their risk management role in this domain is crucial. Bias introduces an unacceptable risk to any organization regardless of where that bias originates. A decision made by an organization's analytic model is a decision made by that entity's senior management team. Internal audit can help management by providing risk-based and objective assurance, advice, and insight. As such, auditors should learn and adapt their methods to meet the challenges organizations face in adopting AI.

ALLAN SAMMY, CIA, CPA, *is the director, Data Science and Audit Analytics, at Canada Post in Ottawa.*

Areas of Deficiency

To inform the audit committee on external audit quality, internal auditors need to be familiar with the PCAOB inspection process and recurring findings.

Elena Isaacson
Heather Losi
Douglas M. Boyle

The U.S. Public Company Accounting Oversight Board (PCAOB) is responding to audit committee requests for more information about PCAOB audit focus areas, stated board member Duane DesParte at the 2018 AICPA Conference on Current SEC and PCAOB Developments in Washington, D.C. Internal auditors are in a unique position to support audit committees in understanding and monitoring these key areas. Internal auditors with a solid understanding of PCAOB expectations and findings can advise audit committees, which have primary oversight responsibility for external audit quality and ensuring the independence and objectivity of the audit firm.

THE PCAOB INSPECTION PROCESS

The U.S. Sarbanes-Oxley Act of 2002 formed the PCAOB, creating an independent auditor oversight institution to protect investors, provide reliable financial reporting, and improve audit quality. The PCAOB performs annual inspections of large audit firms and triennial inspections of small audit firms. A report is issued after every inspection that includes a public portion and, if required, a nonpublic portion.

The public portion describes any significant audit deficiencies and is published on the PCAOB website. Examples of significant audit deficiencies include failure to perform required audit procedures, failure to recognize and address generally accepted accounting principles misapplications, and insufficient testing of the design and operating effectiveness of selected controls. After an inspection, an audit firm may have to modify its audit opinion or prompt the company to issue restated financial statements.

The nonpublic portion of the report addresses deficiencies in the system of quality control. It may include the firm's procedures for assuring independence, the tone at the top, or the firm's internal inspection program. The nonpublic portion of the inspection report becomes public if an audit firm fails to remedy the required quality control deficiencies within 12 months of the report being issued. According to the Center for Audit Quality's (CAQ's) Guide to PCAOB Inspections, the remediation steps that a firm takes depend on the type of underlying quality control issues identified by the PCAOB. Remediation examples include changing the firm's audit procedure manuals and additional training. The PCAOB expects larger firms with complex audits to conduct an analysis of the causes of any identified issues, and adapt its remediation measures to the results of that examination. The CAQ Guide can be helpful to internal auditors by providing guidance on remediation steps and root cause analyses.

Remediation steps that a firm takes depend on the type of underlying quality control issues.

The PCAOB currently is revising the risk-based selection process of audit engagements, which procedures to perform, and how to assess a firm's quality control system and culture, as well as changing the nature, timing, and extent of inspection procedures. In addition, the PCAOB will focus on timeliness and relevance of inspections reports, which will aid investor and audit committee decision-making. Some changes will be implemented as early as the 2019 inspection cycle, said George Botic, PCAOB director of the Division of Registration and Inspections, during a Dec. 12, 2018, speech.

INSPECTION FINDINGS

The three most frequently recurring audit deficiency areas are assessing and responding to risks of material misstatement, auditing internal control over financial reporting (ICFR), and auditing accounting estimates, including fair value measurements (see "PCAOB Audit Deficiency Examples" on page 49), Botic said. The PCAOB highlighted these deficiencies in its 2018 Staff Inspection Brief, Staff Preview of 2018 Inspection Observations, released in May 2019.

Key Deficiency 1—Assessing and Responding to Risks of Material Misstatement Deficiencies related to assessing and responding to risks of material misstatement result in noncompliance with PCAOB Audit Standard (AS) 2301: The Auditor's Responses to the Risks of Material Misstatement and AS 2810: Evaluating Audit Results. The PCAOB's 2017 Staff Inspection Brief, Preview of Observations from 2016 Inspections of Auditors of Issuers, notes that some selected firms were not performing substantive tests robust enough to thoroughly assess fraud risk and other risk factors. The 2017 Inspection Brief specifically mentions risk regarding revenue recognition. The 2018 Inspection Brief highlights the need to test the entire revenue transaction, including comparing company-prepared invoices with related

PCAOB enforcements involving auditors and audit firms **declined 63%** in 2018 compared to 2017, the lowest since 2013, according to Cornerstone Research's Regulatory Actions Involving Accountants.

PCAOB AUDIT DEFICIENCY EXAMPLES

AUDIT DEFICIENCY AREA	NONCOMPLIANCE WITH	AUDIT DEFICIENCY EXAMPLES
Assessing and responding to risks of material misstatement	» AS 2301: The Auditor's Responses to the Risks of Material Misstatement » AS 2810: Evaluating Audit Results	» The auditor did not perform substantive procedures, including tests of details that were responsive to the assessed fraud and other significant risks. » The auditor did not consider relevant audit evidence that seemed to contradict certain assertions in the financial statements. » The auditor did not sufficiently evaluate the presentation of the financial statements, including the accuracy and completeness of the disclosures.
Auditing internal control over financial reporting	» AS 2201: An Audit of Internal Control Over Financial Reporting That Is Integrated With an Audit of Financial Statements	» Some auditors did not assess the nature and relevance of the procedures performed by management during the review. » Some auditors did not appropriately exercise professional skepticism when testing controls, placing reliance on management inquiry. » The auditor did not attain a sufficient understanding of potential misstatement sources. » Some auditors did not adequately examine the controls over completeness and accuracy of system-generated data or reports used in the operation of those controls.
Auditing accounting estimates, including fair value measurements	» AS 2501: Auditing Accounting Estimates	» Some auditors did not fully understand how estimates were established. » Some auditors did not adequately test the significant inputs and assess the significant assumptions used by management.

contractual obligations and product/service delivery and testing invoice amounts to revenue recognition. Firms should presume there is fraud risk associated with revenue and evaluate accordingly. Audit procedures should be designed and performed to address the assessed risks of material misstatement for each relevant assertion of each significant account and disclosure (AS 2301.08). AS 2301.09 emphasizes that when designing the audit procedures, the auditor should:

- Acquire more persuasive audit evidence the higher the auditor's assessment of risk.
- Consider the types of potential misstatements that could result from the identified risks and the likelihood and magnitude of potential misstatement.
- In an integrated audit, plan the testing of controls to accomplish the objectives of both audits simultaneously to obtain sufficient evidence to support the auditor's control risk assessments for purposes of the audit of financial statements and to support the auditor's opinion on ICFR as of year-end.

Some inspections yielded cases where the presentation of the financial statements and completeness of disclosures were not fully evaluated. AS 2810.03 requires external auditors to consider all relevant audit evidence, regardless of whether it appears to corroborate or to contradict the assertions in the financial statements when forming an opinion on the fairness of financial statements.

Internal auditors should work closely with audit committee members to address recurring audit deficiencies by creating and monitoring procedures to ensure appropriate tone at the top, auditor independence, risk assessment of material misstatement, and accounting estimates.

Key Deficiency 2 – Auditing ICFR Deficiencies in this area result in noncompliance with AS 2201: An Audit of Internal Control Over Financial Reporting That Is Integrated With an Audit of Financial Statements. They stem

TO COMMENT on this article,
EMAIL the authors at elena.isaacson@theiia.org

from insufficient testing of estimates related to revenue, business combinations, asset impairments, and reserves. External auditors need to exercise an appropriate amount of skepticism as the 2017 Inspection Brief notes that firms tend to rely too much on management explanation, exhibit bias toward controls being effective, and incorrectly match control testing with control objectives.

The 2018 Inspection Brief describes instances where external auditors' control testing was inadequate.

The 2018 Inspection Brief describes instances where external auditors inadequately tested the design and operating effectiveness of controls, or did not select controls for testing that addressed the specific risks of material misstatement.

AS 2201 establishes a risk-based approach to the audit of internal control. The auditing standard is intended to emphasize the most important matters in the audit of internal control and avoid procedures that are unnecessary to an effective audit. When choosing controls for testing, the external auditor should investigate controls that are imperative to his or her conclusion about whether the company's controls appropriately convey the assessed risk of misstatement to each relevant assertion (AS 2201.39). In addition, AS 2201.42 recommends examining the design effectiveness of controls by verifying whether the company's controls satisfy the control objectives and can effectively prevent or detect errors or fraud. The external auditor should obtain persuasive evidence that demonstrates control effectiveness. As risk increases, so should the obtained evidence.

Staff Audit Practice Alert No. 11: Considerations for Audits of Internal Control Over Financial Reporting presents the application of certain requirements of AS 2201 and PCAOB standards to audits of internal control. This alert offers guidance on the topics of:

- External auditors' risk assessment and the audit of internal control.
- Selecting controls to test.
- Requirements for testing management review controls.
- IT considerations, such as system-generated data.
- Roll-forward of control testing performed at an interim date.
- Using the work of others.
- Evaluating control deficiencies.

Internal auditors possess overall knowledge and understanding of an organization's policies and procedures and are a resource for external audit engagement teams. Internal auditors can assist external auditors in gaining an in-depth understanding of organization processes, transactions, and controls.

Key Deficiency 3 – Auditing Accounting Estimates, Including Fair Value Measurements Deficiencies related to auditing accounting estimates result in noncompliance with AS 2501: Auditing Accounting Estimates. These deficiencies are generally associated with evaluating impairment analyses for goodwill and other long-lived assets, and the valuations of assets and liabilities attained in business combinations. Other instances of auditing deficiencies observed in the 2017 and 2018 Inspection Briefs include revenue-related estimates and reserves, allowance for loan and lease losses, inventory reserves, and financial instruments. The findings demonstrate that the external auditors did not fully understand how estimates were established or did not adequately test the significant inputs and assess the significant assumptions used by management. The 2018 Inspection Brief recognizes that developing these estimates involves

In 2018, more than two in three final PCAOB enforcement actions involved engagement quality reviews, according to Cornerstone Research's Regulatory Actions Involving Accountants.

unobservable inputs, complex valuation models, and subjective judgments; therefore, external auditors should exercise professional skepticism and involve senior members of the team throughout the audit engagement.

AS 2501: Auditing Accounting Estimates offers guidance on obtaining and evaluating appropriate evidence to support significant accounting estimates in financial statements. AS 2501.03 highlights management's responsibility to make the accounting estimates based on subjective and objective factors. Subsequently, management's judgment is required for accounting estimates. This judgment depends on knowledge and experience, as well as assumptions about current and future conditions and courses of action. AS 2501.05 holds management accountable for creating a process for preparing accounting estimates. While the process may not be documented or formally applied, certain steps should be considered:

- » Recognize when accounting estimates are required.
- » Identify factors that may affect the accounting estimate.
- » Accumulate relevant, sufficient, and reliable data on which to base the estimate.
- » Develop assumptions that represent management's judgment of the most likely conditions and events with respect to relevant factors.
- » Calculate the estimated amount based on the assumptions and other relevant factors.
- » Determine that the accounting estimate is presented in conformity with applicable accounting principles and that disclosure is adequate.

According to the PCAOB Inspections Outlook for 2019, inspectors are focusing on the design and operating effectiveness of firms' systems of quality control, assessing and monitoring compliance with independence requirements, and evaluating the audit procedures firms use to identify cyber risks. In 2019, the PCAOB will look at the use and development of firm software audit tools to consider whether firms are using these tools effectively and applying due care, including professional skepticism. It also will assess auditors' responses to risks associated with digital assets, such as cryptocurrencies, initial coin offerings, and use of distributed ledger technology. In addition, the PCAOB will focus on client acceptance and retention decisions, resource management, and planned audit procedures.

Business combinations also are a recurring item appearing under internal control testing deficiencies.

Revenue recognition is identified as an area of concern in all deficiency areas, so firms need to pay particular attention to assessing risk related to revenue, designing tests of revenue control, and evaluating revenue estimates. Business combinations also are a recurring item appearing under internal control testing deficiencies as an area affected by economic risk and a financial reporting concern. The 2017 Inspection Brief says that firms need to go beyond management inquiry by testing controls related to other controls, gaining an understanding of the basis of client estimates, and using professional skepticism.

The 2018 Inspection Brief also reports that some audit firms failed to communicate to audit committees significant risks and changes to those risks. Strong communication with external auditors can help audit committee members recognize "the external and company-specific factors considered by the auditor in assessing whether all significant risks have been identified," as well as assist audit committees in exercising their oversight roles. Internal auditors should take part in communication with the audit committee, as well as external auditors, on any identified PCAOB deficiencies to ensure that all parties involved in the audit engagement have a clear understanding regarding remediation actions.

INTERNAL AUDITOR AS ADVISOR

The audit committee has a joint oversight role with the PCAOB when it comes to audit quality and engaging in dialogue concerning deficiencies and the PCAOB inspection process. It needs to understand the PCAOB's recurring audit deficiency findings when fulfilling its supervision responsibility for audit quality and ensure the independence and objectivity of the external audit firm. Internal auditors with sound knowledge of this process can inform and advise the audit committee in this area so it can better fulfill this role. Ia

ELENA ISAACSON, *is an accounting instructor at Siena College in Loudonville, N.Y.*

HEATHER LOSI, CPA, *is visiting assistant professor at the State University of New York at Oswego.*

DOUGLAS M. BOYLE, DBA, CPA, CMA, *is accounting department chair and associate professor at the University of Scranton in Penn.*

Don’t manage RISK – Manage VALUE

Marinus de Pooter

Risk management’s traditional focus on adversity is changing. The Committee of Sponsoring Organizations of the Treadway Commission’s (COSO’s) 2017 *Enterprise Risk Management (ERM)–Integrating With Strategy and Performance* framework now refers to *risk* holistically as “the possibility that events will occur and affect the achievement of strategy and business objectives.” With “adversely” removed from the definition, a risk is no longer something that must be prevented from happening. In addition, the framework no longer speaks of *risk management* as a separate process, but defines it in terms of “culture, capabilities, and practices.”

The updated COSO ERM framework and the International Organization for Standardization’s ISO 31000: Risk Management standard present great opportunities to replace the term *risk management* with *value management*. According to both standards, managing risk is all about creating and protecting value. However, they retain the term *risk management*.

Business activities always involve uncertainty. To increase success, leadership teams have to take advantage of opportunities and limit threats. Ultimately, they want to increase the certainty they will achieve their objectives and will not get what they do not want. For that reason, organizations need a

BILLION PHOTOS / SHUTTERSTOCK.COM

Changing risk standards pave the way for organizations to bring their experts together to pursue opportunities and cope with threats.

pragmatic approach to keep key stakeholders satisfied by realizing value for them.

The value management approach offers intriguing opportunities for internal auditors because it focuses on the quality of decision-making within the organization. Internal audit can help the organization by assessing to what extent decision-makers possess the right competence and integrity to reconcile dilemmas caused by the conflicting interests of stakeholders.

BECOMING FUTURE-PROOF

Being future-proof requires an organization to continually create and protect value for its core stakeholders. However, terms such as *value*, *result*, *success*, and *improvement* only gain substance through the meaning that stakeholders attach to them. Stakeholders look at an organization from their own perspective. Based on their interests, they find certain things valuable such as innovation, punctuality, privacy, safety, compliance, integrity, efficiency, and continuity.

Future viability is about anticipating what might happen. The leadership team wants to know where the

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

organization is expected to end up and to what extent this differs from what the organization's core stakeholders expect. Is the organization on the right track? Or is there a real chance that it will not achieve its objectives? In that case, is the organization taking appropriate measures? Conversely, the organization may be exceeding expectations, because it is able to deal well with uncertainty.

BRINGING EXPERTS TOGETHER

Strategic, tactical, and operational decisions imply making choices and balancing potential pros and cons. Working standards and methods are intended to guide the decision-makers in the right direction. Determining these rules is the domain of specialized departments such as business continuity, compliance, control, information security, privacy, quality, and safety. Typically, all these functions conduct risk assessments, build control frameworks, and produce management reports, which easily can lead to functional silos and value destruction in practice.

Conventional risk management is a flawed concept (see "Value Management and Internal Audit" on page 55). Instead of having a separate program, function, or committee for managing risks, organizations should focus on connecting the functional experts. Generating and preserving value is dependent on these specialists collaborating to assist decision-makers at all levels with seizing opportunities and limiting threats. As an independent advisor, internal audit can help reduce organizational complexity and silo-thinking.

To connect the experts effectively, leadership teams should seek answers to five key questions. These basic business questions are the building blocks for the practical analyses that leaders can carry out for a separate business process, project, department, branch, division, value chain, or the entire organization.

Answering each of these questions requires making choices and balancing opportunities and threats. For example, implementing extensive control frameworks (part of the "how" question) may send the message to those involved that they have flawed judgment or lack integrity. Internal audit should independently assess to what extent leaders answer the questions satisfactorily.

> Value management hinges on the effectiveness of governance.

Who Can Decide? Value management hinges on the effectiveness of governance: Who is authorized to make which choices? This applies to allocating resources both to daily operations and continuous transformation. The individual responsible for achieving formulated objectives also should be able to decide how best to deal with relevant opportunities and threats. This can be done by optimizing the associated business processes and controls.

A prominent and practical issue concerns the mandate of the experts in the organization's staff departments. To what extent are they allowed to prescribe working standards to their colleagues or are they only expected to provide advice? How does the leadership team ensure that the staff specialists keep the line managers in focus? On the other hand, how can leaders prevent the experts from exaggeration caused by enthusiasm? An example is information security specialists who produce unworkable policies and procedures.

What Do We Do? Each leadership team benefits from having an integrated overview of the clustered activities of everyone involved within their entity. This structured summary of current tasks shows the organization's common playing field. The overview of managerial, primary, and supporting processes provides insight into all relevant transaction flows and volumes. It also forms the basis for the IT application landscape for processing the transactions. Hence, it is the foundation for information management, business intelligence, and forecasting. Do those in charge have the right information for making balanced decisions? The advantages of better insight into who does what are evident in initiatives such as integration projects.

Why Do We Do What We Do? The organization's success is determined by the extent to which its core stakeholders are satisfied. They are primarily interested in how the leadership team's performance affects their interests. That is why the stakeholder analysis is essential. If all goes well, the team's ambitions fit in with the value that the organization wants to create and protect for specific stakeholders. This value is expressed in the organization's mission, vision, and strategy, and is translated into concrete success factors, objectives, and indicators. Using clear tolerances for the key indicators and preparing regular forecasts provide ample input for timely adjustment. If the estimated outcomes are not within the bandwidths, the two options are to adjust the controls or to inform key stakeholders that they must accept revised tolerances.

How Do We Do What We Do? To apply judgment, decision-makers need a framework and rules such as working standards and methods. The practical details of these rules are laid down in the charters, policies, guidelines, procedures, protocols, and work instructions.

59% of finance executives say the volume and complexity of risks have mostly changed over the past five years, reports The State of Risk Oversight survey by AICPA and the ERM Initiative.

VALUE MANAGEMENT AND INTERNAL AUDIT

Embracing the value management approach is different from advocating conventional risk management practices. Here are examples of what will change for internal auditors:

- Instead of focusing on the organization's biggest vulnerabilities, internal audit holistically focuses on assessing the quality of management. Decisions made when planning, executing, monitoring, and improving business activities always have potential positive and negative effects on the interests of key stakeholders.
- Instead of believing the organization should have a separate risk management process, function, or system, internal audit focuses on the organization's capabilities to become future-proof. Propagating lots of separate risk terms, such as risk manager, risk culture, risk appetite, and risk report, may not lead to the realization of business objectives.
- Instead of seeking to assess whether what COSO's 2017 ERM framework calls the second line of accountability fulfills its responsibilities for overseeing performance and conformance, internal audit assesses the competence and integrity of decision-makers at all levels of the organization.
- Instead of unilaterally focusing on money, internal audit recognizes that *value* implies more than cash, profit, stock price, and dividend. Key stakeholders have different interests and attach value to divergent matters.
- Instead of embracing in-control statements oriented to the past, internal audit realizes that the key question is to what extent decision-makers at all levels of the organization are capable of creating and preserving value for key stakeholders in the future.
- Instead of assuming that the future is makeable and perfectible through risk analyses, risk and control matrices, and control testing, internal audit acknowledges that the world is volatile, unpredictable, complex, and ambiguous, requiring a considerable degree of agility and flexibility.
- Instead of assuming that risk management should be a separate item on the agenda for team meetings, internal audit emphasizes that each of the items is about effectively dealing with opportunities and threats.

Clear working arrangements streamline decision-making, facilitate work hand-off among colleagues, and provide a clear reference for audits. The "how" question is about autonomy. For example, to what extent are subsidiaries allowed to make their own rules?

The decisive factor in the "how" is the organization's culture. Is it characterized by managers setting the examples? Are decision-makers willing to face the possible consequences of their choices? Is it acceptable to challenge the assumptions in overly ambitious plans?

What Can We Improve? A continuous improvement program helps the leadership team focus on what really matters. When asked about the "best improvements," people typically mention situations where the risk exposure is bigger or the chance taking is smaller than desired. The necessary improvements are usually about better designing, implementing, applying, and monitoring the organization's working methods and standards. These renovations explicitly deal with the competencies of those involved—not only their professional knowledge and skills, but especially their personal leadership qualities.

A continuous improvement program can enable the team to identify, prioritize, and realize improvement initiatives. The better the information management is and the more that employees feel free to report issues, the sooner trends can be identified.

VALUE FOR STAKEHOLDERS

Conventional risk management can easily turn into a separate, illusory, and compliance-driven system. Alternatively, value management is an integrated approach that can give leadership teams a single platform for all common types of management. It can help decision-makers identify, prioritize, and realize relevant improvements that are needed to satisfy their core stakeholders.

MARINUS DE POOTER, CIA, CMA, CFM, CRMA, *is owner of MdP | Management, Consulting & Training in Deurne, Netherlands.*

Board Perspectives

BY MATT KELLY

BOARD PROBLEMS

With stakeholders' growing emphasis on corporate culture, boards could benefit from ethics expertise.

DAVID GREENBERG

OWEN BAILITZ

TRACY ATKINSON

Audit committees have a problem: They have too many problems. More precisely, they have too many *types* of problem—too many types of corporate misconduct to consider these days, because the definition of *misconduct* has expanded dramatically in the last 15 years.

That raises questions about the expertise audit committees need, and whether corporate boards have enough of it. Quite simply, if society wants corporations to exercise a sharper sense of ethics and moral responsibility, do we need more ethics and compliance officers serving on boards?

"It's undeniably true," says David Greenberg, former chief compliance officer (CCO) at tobacco manufacturer Altria and an audit committee member of International Seaways, a New York Stock Exchange-traded oil and gas tanker business. The definitions of *corporate misconduct* are expanding, he says, and the consequences of it are deepening. "Put those two things together, and it's a recipe for needing more of that experience."

A recent regulatory enforcement example demonstrates the point. Cognizant Technologies, an IT outsourcing firm, had been accused of violating the U.S. Foreign Corrupt Practices Act when two of its senior executives orchestrated a US$2 million bribe to government officials in India. The involvement of two senior executives would typically leave Cognizant unable to avoid criminal prosecution, according to U.S. Department of Justice (DOJ) policy. Yet when regulators settled the case in February, the DOJ did decline to bring any criminal charges. Prosecutors later said why: "The company voluntarily self-disclosed the conduct within two weeks of when the company's board learned of it."

Confessing egregious corporate misconduct is unquestionably the right thing to do. Still, confession is a big request—especially when doing so invites potentially serious legal and financial consequences, such as monetary penalties or a corporate criminal charge. So Cognizant's decision to disclose its trouble immediately, without any certainty of favorable treatment, is all the more impressive.

Where did that ethical commitment come from? It's worth noting that Cognizant's audit committee chair at the time was Maureen Breakiron-Evans, who worked as general auditor of Cigna in the 2000s. Also on the committee was Leo Mackay, head of ethics and internal audit at Lockheed Martin. Both still serve on Cognizant's board.

Beyond Financial Expertise

Under the U.S. Sarbanes-Oxley Act of 2002, the audit committee of a publicly traded firm needs at least

READ MORE ON STAKEHOLDER RELATIONS visit InternalAuditor.org

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

one designated "financial expert" to help the audit committee police against financial fraud. When the act was passed, that might have been enough of a kick in the corporate rear to take internal control more seriously. Today, a strong control environment has become much more important, to address all sorts of issues. Regulators don't just want swift corrective action; they want strong *preventive* action. Customers, business partners, or even self-appointed social justice warriors prowling Twitter— all want to see ethical culture taken seriously, translated into tangible policies, controls, and actions.

"A true auditor on the board, or a true employee relations or corporate compliance person, is important because what's falling to the audit committee to investigate—it's gone way beyond what audit committee charters originally said," says Owen Bailitz, a former risk management and audit quality partner with RSM, who now serves on the audit committee of the American Board of Medical Specialties. "You're basically expanding the definition of risk."

Audit executives could perceive all of this as a virtuous circle. Yes, data analytics captures data about business process outputs, to identify anomalous events or excessive risks. Those insights let directors draw conclusions about how the enterprise is working. We still need the other half of the circle: using those insights to change policy, procedure, and culture, so business processes can stay within ethical parameters more easily. That's the improvement society wants to see.

"Across stakeholders, there's been more engagement with boards on this discussion. Ethics and culture are topics that are relevant to the full board and every committee of the board," says Tracy Atkinson, audit committee chair of defense and aerospace systems provider Raytheon Co. "Having someone who lives and breathes this on the board adds to the dialogue in a new way." Atkinson would know; she is executive vice president and CCO at financial services company State Street Corp.

We see that increased engagement in various ways. For example, the Edelman Trust Barometer, which surveys more than 33,000 people worldwide about their trust in institutions, recently found that 76% say their employers should "take the lead on change" for issues such as sexual harassment, the environment, and discrimination. And 71% said it's critical for their CEO to respond to challenging issues.

Then there are regulatory pressures. For example, a board might find itself saddled with a corporate integrity agreement where the audit or risk committee has to certify compliance with the terms. Having a compliance or internal control expert on the board would make that an easier exercise.

Those are examples at the macro level. At the micro level, chief audit executives (CAEs) have this: The *Politics of Internal Auditing*, a 2016 IIA study, found that 55% of audit executives had been asked to suppress unwanted findings during their career. That tells us two things. First, that internal audit executives are well-acquainted with the threats of bad ethical culture; and second, that CAEs would be well-suited to serve on boards someday—because they (like CCOs) have seen poor ethical behavior up close, and it's their job to uncover and eradicate bad behavior anyway, whatever the consequences.

That skill, of identifying the ethically correct step, taking it, and defending it, will only become more important. As Greenberg says, questions about disclosing misconduct, and whether voluntary disclosure is worth it, can be quite difficult. "You need people with some experience to overcome that."

Meanwhile, the Reality

As desirable as ethics, audit, and compliance perspective on the board might be, practical limitations abound. Boards are still desperate to recruit women and minorities; some jurisdictions now require specific quotas for female directors. Boards also are desperate for cybersecurity expertise. And yes, foremost, boards want to recruit current or former CEOs, chief financial officers, and chief operations officers—people who understand the intersection of strategy, operations, and finance.

That leaves few open seats for other governance expertise. So boards might not rush to the idea of recruiting CAEs or CCOs, unless they're particularly committed to foresight. As Bailitz put it: "You need to have a change of mindset among the chairpersons of these boards, to say, 'We lack this expertise, and it's something we need.'"

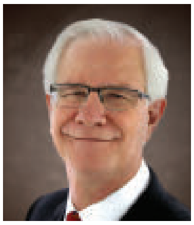
The push for cybersecurity expertise is a good parallel. Most executives, audit committees members included, understand cybersecurity at a reasonable level—what it is, why it's important, and what it should achieve. But they don't understand how to assess it, improve it, or weave it through all of an organization's operations. Only a cybersecurity expert does.

Ethical culture is a lot like that, Atkinson says. Boards might believe they can master ethics and culture because it seems like a nontechnical issue, but introducing an audit or compliance executive can sharpen the board's perspective in new ways. "It's a mindset," she says. "Having compliance and ethics as your subject matter domain, and bringing that to the board, further serves to emphasize" where ethics and the control environment might need attention.

So will boards put more audit and compliance professionals on the audit committee or even some other board committee? Will recruiters start calling CAEs and CCOs? That's hard to say, but it's not just self-interest for CAEs to want that to happen. This is what the future of boardroom problems looks like, and the future has a habit of arriving eventually. Ia

MATT KELLY *is editor and CEO of Radical Compliance in Boston.*

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



BY J. MICHAEL JACKA

AUDITOR, AUDIT THYSELF

Practitioners need to turn audit techniques on themselves and examine their department's culture.

How many times have you heard someone ask, "Who audits the auditors?" It's a question frequently posed to practitioners, and for many of us there is a ready answer: "We go through an external assessment every five years to attest that we conform with the *International Standards for the Professional Practice of Internal Auditing*."

That's all well and good, and worthy of the associated bragging rights. But the audit department that assumes the pursuit of audit quality ends with conformance is fooling itself, its audit staff, and its organization. Conformance with the *Standards* should be considered a given—the audit department that wants to be seen as a trusted advisor and an invaluable stakeholder resource must hold itself to an even higher standard. The best way to achieve that is to turn audit techniques on our own operations—review our efficiencies and effectiveness; ensure we understand the risks to our objectives; and evaluate how well our strategies, objectives, and controls work together toward success.

There may be no more impactful place to start than taking a good, hard look at the culture within the department. Organizational culture is a major topic for board members, executives, and other stakeholders—it is the foundation for success and at the root of almost anything that goes wrong.

Internal audit is not immune. Success for an internal audit department relies on any number of elements, but foundationally sustained success cannot be achieved without the hallmarks of a healthy culture, including honesty, open communication, accountability (at all levels), and trust.

I have worked with audit departments that bragged about having "passed" their external quality assessment review, but subsequently learned through private conversations about the auditors' discontent, disaffection, and distrust. The auditors reveal they don't get the support they need, they cannot be honest with those in charge, they work in an atmosphere of negative competition, and, overall, they are working in an unhealthy environment.

Internal audit leaders should take steps to ensure their rose-colored perception of the department's culture is real. If they conduct employee satisfaction surveys, the results should be taken seriously, not dismissed as the feedback of a few malcontents. Human resources should be used as a partner to better understand what is really going on in the department. But most importantly, leadership should be willing to talk with the staff. If audit leaders think such discussions will not provide real information, or if they are convinced it is a waste of time, then, yes, there is a problem.

And one final note. If you are not in a position of authority but find yourself in a toxic culture, you can choose to live in pain or just escape. However, the more courageous tact may be to step forward, pointing out the deadly practices potentially destroying the department. Ia

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

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

THE HEALTHY CORPORATE CULTURE

CAEs increasingly are being asked to assess, monitor, and report on the health of the organization's culture.

CHARMIAN SIMMONS
Risk Market
Development Manager
Refinitiv

ESI AKINOSHO
Principal, Global
Advisory Internal
Audit Leader
Ernst & Young LLP

How does an organization develop and maintain a healthy corporate culture?

SIMMONS Implementing a clear mission and company values sets the tone and messaging from the top, and specifying the organization's desired risk culture in a way that aligns with these values helps solidify the corporate culture. Establishing a collaborative, open communication approach creates a comfortable work environment and is the best way to maintain a culture where people feel valued, respected, and empowered to offer ideas and make good decisions. Having a leadership team that believes in this approach, lives the mission/values, and knows what employees value contributes to an atmosphere where ideas are celebrated and rewarded, which can lead to a more efficient and productive organization.

AKINOSHO First, we need to define a *healthy* culture. A healthy corporate culture is a) connected to the company's purpose and strategy; b) positive, inspiring, and engaging for employees who live it, customers who experience it, and shareholders who realize returns from it; and c) strong, consistent around the world, and not overly dependent on the effectiveness of a local leader. Developing a healthy corporate culture takes time, focus, and direction from leadership, as well as level support from key functions to help champion that desired culture. A top-down and bottom-up approach is key in not only the development of a healthy culture, but also in sustaining and fostering changes in it.

What are the top risks to a healthy corporate culture?

AKINOSHO Risk culture connects the overall organizational culture to specific behaviors set along a defined risk framework. It speaks to culture in terms of the three lines of defense and guides how leadership monitors and responds to cultural stress and the risks of an unhealthy culture. Risks relating to corporate culture include a degraded tone at the top, lack of accountability, and minimized transparency. Cultural stress often takes the form of compliance issues, control failures, audit issues, or poor employee performance, and the typical root cause is often a breakdown in trust. Trust can be the biggest risk or asset to a healthy corporate culture, and the erosion of trust can be hard to control and even harder to earn back. By aligning the corporate culture and pulling certain cultural levers, trust can become the driving force for creating a shared vision and turning that vision into value.

SIMMONS First and foremost is culture risk, itself. Well-known corporate scandals related to harassment, fake accounts, accounting errors, and misconduct often are symptoms of culture

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

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

issues and heighten the profile of culture risk as a growing liability for organizations. Culture risk management should be treated as an integrated process of oversight and monitoring that addresses strategy, performance, and risk, and aligns company values, goals, behaviors, and systems with favorable impacts both internally and externally. Other top risks that can affect a healthy corporate culture include financial, operational, market, and reputation risks. The particulars of each risk, such as ranking, priority, and specific factors, will vary by company/industry/geography and by the awareness level of underlying problems, mitigations, and ongoing monitoring. Some symptoms and behaviors that influence these risks include financial underperformance, inconsistencies in business/personnel performance, communication that leads to misunderstanding, unhealthy comparisons and gossip, demoralized employees, customer backlash, and the feeling of destroyed value.

What are the indicators of a weak or failing corporate culture?

SIMMONS Indicators can be broadly classified into top-down and bottom-up. Indicators from a top-down business perspective include inconsistent financial and operational success and being perceived by the public and personnel as not conducting business activities with honesty and integrity. From a bottom-up personnel perspective, indicators may include lack of motivation; overwhelming frustration, such as fear of retaliation in speaking out, not being listened to, or pressured to meet unrealistic internal deadlines; poor customer relations; pending investigations; lack of efficiency or ideas; and lack of innovation. These indicators may be noticed by management, personnel, and internal audit, though one must be open and conditioned to seeing the signs to be receptive to raising the matter and taking active and visible action.

AKINOSHO A weak culture can be characterized by inconsistent programs that deviate from the common goal and vision. Functional groups, including internal audit, that have different strategic objectives or have pockets of opposing forces will create stress within an organization's operating model and increase the risk of compliance issues, failure to adhere to policies, and internal control breakdowns. Lack of leadership or misaligned tone at the top can hold an organization back and put it at risk for cultural issues. Today, many of these issues are coming to light in very public settings, which is why boards and audit committees are turning to internal auditors, the third line of defense for culture risk management, for insight.

What should a formal culture risk management program look like?

AKINOSHO A formal culture risk management program is embedded throughout all three lines of defense, with the first line implementing the mechanisms to drive culture, the second line taking responsibility for defining the risk culture framework and monitoring effectiveness, and the third line performing independent culture assessments to monitor culture throughout the execution of the audit plan.

SIMMONS Recent incidents and news headlines linked to "problematic culture" lead me to say there is no one-size-fits-all program; however, a culture risk management framework should comprise certain key elements that cover all aspects of culture and can be improved and measured over time. First, *governance*—the mission, values, ethics, policy, board, leadership, strategy, behaviors, and a common understanding of what's expected. Second, *relationships*—transparent, honest, and nonthreatening leadership, communications, collaborations, and accountability. Third, *environment*—the workplace provides for comfortable, productive, inspired, responsive, innovative, rewarded, trusted, engaged employees and supports organizational effectiveness. Fourth, *motivation*—a fair values system exists surrounding performance, incentive, reward, continuous learning, and clarity of purpose.

How does a dynamic, agile workplace affect corporate culture?

SIMMONS One affects the other and impacts the success of both. Many organizations want to be more agile to respond to the demands of customers, the digital economy, and rapidly changing marketplaces; however, most don't appear to have the culture to support this. Being dynamic and agile means being able to quickly and easily adapt to constant change. A workplace environment like this needs to balance the mindset of change with tools, systems, and processes that support an agile approach and allow the four key culture elements mentioned previously to thrive and positively influence behaviors around cooperation, fast decision-making, experimentation, innovation, empowerment, sustainability, and effective cross-functional teamwork.

AKINOSHO As companies adopt more dynamic and agile approaches and workplaces, they must be aware that the shifting operating models and transient nature of the workforce will have an impact on culture and can even present new risks. When unsuccessfully implemented, an agile operating model can cause a lack of vision or uncertainty in objectives for employees. This cultural stress will work against the achievement of objectives and strategy. Alternatively, an agile workplace can strengthen and foster an existing healthy culture and better advance the people agenda in areas such as development, employee retention, and workforce management. Ia

IIA Calendar

IIA CONFERENCES

www.theiia.org/conferences

JULY 7–10
International Conference
Anaheim Convention Center
Anaheim, CA

AUG. 12–14
Governance, Risk & Control Conference
The Diplomat
Fort Lauderdale, FL

SEPT. 16–17
Environmental, Health & Safety Exchange
Washington Hilton
Washington, DC

SEPT. 16–17
Financial Services Exchange
Washington Hilton
Washington, DC

SEPT. 18
Women in Internal Audit Leadership Forum
Washington Hilton
Washington, DC

SEPT. 20–22
Internal Audit Student Exchange
Rosen Centre Hotel
Orlando, FL

OCT. 21–23
All Star Conference
MGM Grand
Las Vegas

IIA TRAINING

www.theiia.org/training

JUNE 3–12
Critical Thinking in the Audit Process
Online

JUNE 3–14
CIA Exam Preparation – Part 1: Essentials of Internal Auditing
Online

JUNE 4–7
Multiple Courses
New Orleans

JUNE 17–26
Building a Sustainable Quality Program
Online

JUNE 18–21
Tools & Techniques III: Audit Manager
St. Louis

JUNE 18–26
CIA Exam Preparation – Parts 1, 2, & 3
Lake Mary, FL

JUNE 24–27
Vision University
Boston

JULY 8–19
CIA Exam Preparation – Part 3: Business Knowledge for Internal Auditing
Online

JULY 15–24
Cybersecurity Auditing in an Unsecure World
Online

JULY 16–19
Multiple Courses
Orlando

JULY 30–AUG. 2
Multiple Courses
Denver

AUG. 6–9
Multiple Courses
Los Angeles

AUG. 6–15
Enterprise Risk Management: A Driver for Organizational Success
Online

AUG. 12–21
Audit Report Writing
Online

AUG. 13–16
Multiple Courses
Chicago

AUG. 13–22
Operational Auditing: Influencing Positive Change
Online

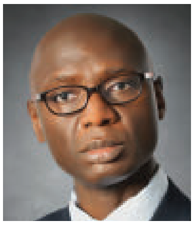
AUG. 19–28
Critical Thinking in the Audit Process
Online

NE/JULY/AUGUST/SE

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 solomon.simutowe@theiia.org



BY SOLOMON CHIEF SIMUTOWE

VALUE THROUGH QUANTIFICATION

Showing the net benefits of implementing audit recommendations can be a great service to clients.

A review of publicly available internal audit reports shows that most include qualitative assessments of value addition, even where quantitative assessments seem possible or advantageous. In fact, some audit reports show that an assessment of the audit recommendations' net benefits had not been performed at all. Without a quantitative assessment, in many instances auditors cannot be certain their recommendations add rather than destroy value. While qualitative assessments are useful for analyzing simple issues, they could be misleading if used for complex, high-risk, or novel situations. Internal auditors should quantify recommendations applied to these types of areas—especially when aimed at improving processes or aligning with best practices.

Without quantification, auditors run the risk that seemingly beneficial audit recommendations may in fact be ill-advised. By using a qualitative assessment, especially one that is not adequately documented, an auditor could miss interdependencies and ignore relevant costs, thereby overstating net benefits. For example, consider a recommendation intended to improve transaction processing efficiency through a system enhancement. On the surface, such a recommendation would appear to create value. But what if over the lifetime of the system, estimates of benefits associated with processing-time savings totaled less than the cost of implementing and maintaining the enhancement? This drawback would not be apparent without quantification of net benefits.

Quantification also provides an effective way of getting buy-in from audit clients. Often, client inertia or resistance increases if recommendations provide questionable or unconvincing value. Clients may raise legitimate concerns about why they should dedicate scarce resources to recommendations whose value is unclear. By demonstrating quantitatively that the value addition is positive, audit client buy-in would be more forthcoming.

Additionally, quantification can help auditors provide assurance when recommendations involve unchartered waters for clients. In other words, audit recommendations may involve changes in areas that are unfamiliar to the client, such as new business processes or initiatives. Gaining reliable insight into the real net benefits can be difficult using only qualitative assessments, making quantitative data in such instances a near imperative.

Lastly, with quantified net benefits of their recommendations, auditors can better demonstrate the value of their work by tracking benefits realized post-implementation. Auditors could harvest the quantified data showing the individual or aggregated impacts of their recommendations on processes, functional areas, or whole entities.

Under the right circumstances, a strong case exists for demonstrating the value of audit recommendations quantitatively. When used appropriately, quantification can shine a bright light on audit benefits, rather than leaving clients in the dark. Ia

SOLOMON CHIEF SIMUTOWE, CIA, CRMA, CISA, FCCA, *is a senior internal auditor at an international organization in The Hague, Netherlands.*

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