Ia
INTERNAL AUDITOR

DECEMBER 2017

INTERNALAUDITOR.ORG

Trust and the Third Party

The Rewards of Nonfinancial Auditing

An Agile Audit Function

Are Your Recommendations Being Addressed?

AI HAS ARRIVED

Artificial intelligence is here, there, and everywhere—it's imperative that auditors understand its implications.

Get $500 OFF Training and FREE Audit Intelligence Suite Bundle.

The Audit Intelligence Suite (AIS) is a premium solution that lets you benchmark your audit activity, assess your team's skills, and survey your key stakeholders. Until March 31, 2018, participants who complete all three components will receive the AIS bundle* free, AND get a $500 discount on On-site Group Training. Our training consultants will use the AIS results to customize a training program to address any gaps in your audit activity.

For more information, visit www.theiia.org/AISandOnsite

* The Audit Intelligence Suite Bundle includes a Benchmarking, Skills Assessment, and Stakeholder Report. The discount may not be combined with other offers.

The Institute of Internal Auditors

Pentana Audit

Don’t allow your Audit Team to be forced into Checkmate

Let Ideagen help your audit team plan their next move with Pentana Audit

Find out why Pentana Audit should be your Audit Team’s next move

ideagen.com/**pentana**

ideagen

+44 (0)1629 699100 | info@ideagen.com

Copyright © 2017 Ideagen PLC

Ideagen are a representative vendor in Gartner’s 2017 Market Guide for Corporate Compliance and Oversight Solutions

Connecting the World Through Innovation
Network | Learn | Innovate | Lead
DUBAI, UAE, 6–9 MAY 2018

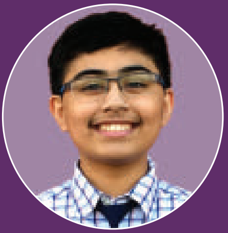
Join Industry Leaders in Dubai

Register today and take advantage of this amazing opportunity to learn from and network with peers from around the globe. Experience dynamic sessions highlighting solutions to help audit leaders worldwide keep pace with changes in technology and techniques.

100+ Speakers From Around the Globe

70+ Sessions in 10 Educational Streams

2,500+ Audit Industry Practitioners & Providers From 100+ Countries



NEW CONFIRMED SPEAKER

Tanmay Bakshi, Neural Network Architect, Honorary IBM Cloud Advisor

Open Source Development: Information Security and Technology Auditing

This 14-year-old phenomenon has taken the technology world by storm. His expertise in neural networks and artificial intelligence is transforming the way technology is used to overcome obstacles in fields like healthcare.

Register Today
ic.globaliia.org

THE INSTITUTE OF INTERNAL AUDITORS
IIA INTERNATIONAL CONFERENCE
DUBAI, UAE / 6-9 MAY 2018
DUBAI 2018

2017-1139

Ia
INTERNAL AUDITOR

DECEMBER 2017 VOLUME LXXIV: VI

FEATURES

Ia Download on the App Store GET IT ON Google play DOWNLOAD the Ia app on the App Store and on Google Play!

FOR THE LATEST AUDIT-RELATED HEADLINES visit InternalAuditor.org

mkinsight

Audit Management Software

☑ No Gimmicks

☑ No Metaphors

☑ No Ridiculous Claims

☑ No Clichés

Find out more at **www.mkinsight.com**

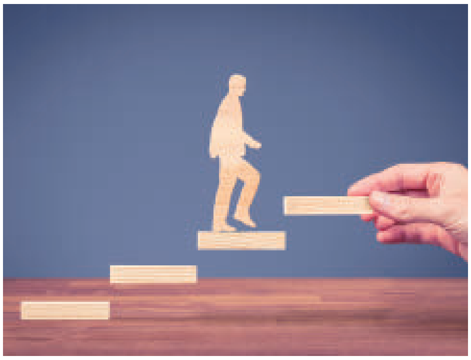
Trusted by Companies, Governments and Individuals Worldwide.

Ia
INTERNAL AUDITOR

DECEMBER 2017 VOLUME LXXIV: VI

DEPARTMENTS

ONLINE InternalAuditor.org



The Value of Mentorship Three of *Internal Auditor's* past Emerging Leaders describe their experiences with mentors and the impact these individuals have had on their careers.

Top Articles of 2017 See which *Internal Auditor* articles were the most popular this year, based on visits to InternalAuditor.org.

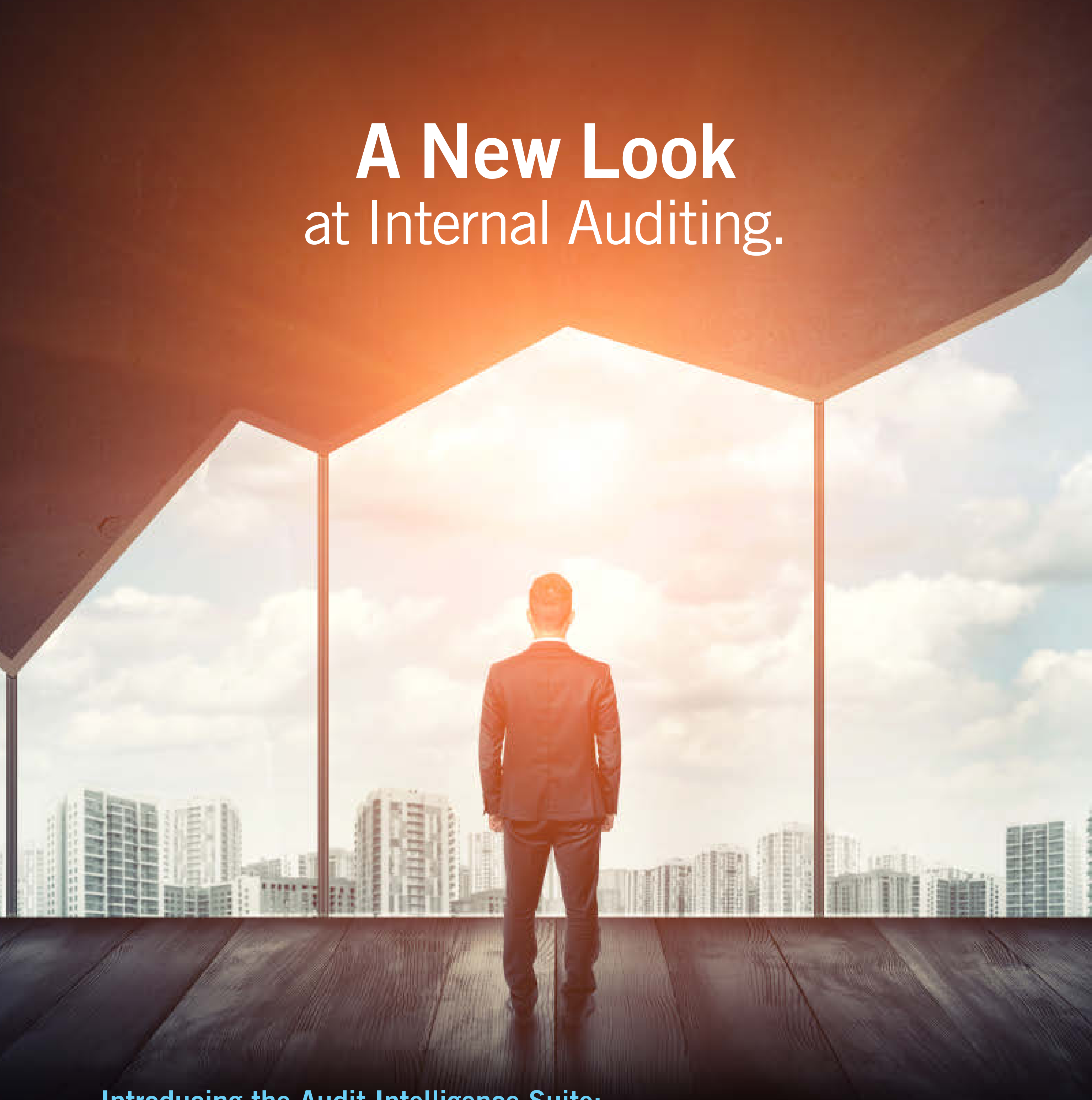
Card Abuse Runs Rampant Australian government agencies are reportedly plagued by unauthorized credit card use. Fraud expert Art Stewart examines the alleged abuse.

AI in the Real World Discover how companies are putting artificial intelligence to use, including applications for gathering customer information, in an extended version of our cover story.

Find us on Facebook

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

IMAGES: COVER, MICK WIGGINS; TOP, MICHAEL D BROWN / SHUTTERSTOCK.COM; RIGHT, JIRSAK / SHUTTERSTOCK.COM



Introducing the Audit Intelligence Suite:

Benchmark | Assess | Survey

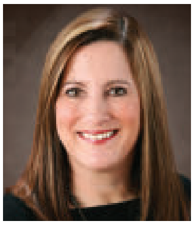
Benchmark your audit function, assess your team, and survey your key stakeholders. Once you know the results, you will be in a better position to improve your audit function.

Learn More

www.theiia.org/AuditIntelligenceSuite

The Institute of Internal Auditors

AUDIT EXECUTIVE CENTER®



THE ROBOTS ARE COMING... FOR MY FAMILY

My husband and I had lunch with our 19-year-old college sophomore last weekend. He's majoring in IT. I tried to persuade him to take a look at artificial intelligence (AI) as a career option. After all, it will likely be taking over his family's jobs—and we'll need him to support us.

You see, his dad is an accountant, one of "The Five Jobs Robots Will Take First," according to *AdAge* magazine. "Robo-accounting is in its infancy," the article explains, "but it's awesome at dealing with accounts payable and receivable, inventory control, auditing, and several other accounting functions that humans used to be needed to do."

Another of the top five jobs robots will take according to *AdAge*? His mother's. Given the fact that, last year, IBM and marketing company The Drum announced that Watson, IBM's AI tool, edited an entire magazine on its own, my days in publishing may, indeed, be numbered.

And, finally, there's his sister. She plans to follow in the footsteps of a long line of teachers in our family—unfortunately, it may be the end of the line. IBM's Teacher Advisor With Watson "is loaded with the lesson plans and proven strategies [needed] to teach across a variety of elementary grade levels and student abilities," reports 3BL Media. "And because it's cognitive, Teacher Advisor will get smarter—and better—with training and use."

According to Harnessing Automation for a Future That Works, a McKinsey Global Institute Report, "almost every occupation has partial automation potential." The report estimates that about half of all the activities employees are paid to do in the world's workforce could be automated by adapting current technologies.

The good news, according to McKinsey, is that less than 5 percent of occupations are candidates for *full* automation. Take internal auditing, for example. In this month's cover story, "Audit in an Age of Intelligent Machines" (see page 24), David Schubmehl, research director for Cognitive/AI Systems at IDC, says "There's going to be tremendous growth in AI-based auditing, looking at risk and bias, looking at data."

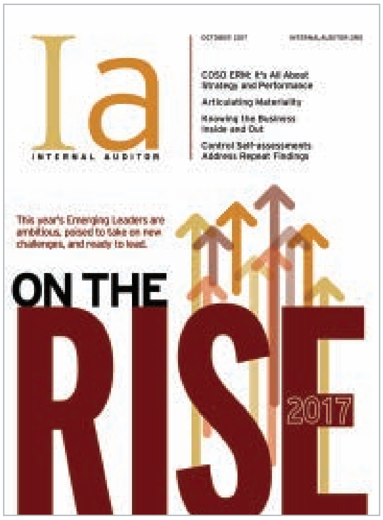
So maybe there's hope after all. Maybe these technologies will just supplement and enhance our jobs. Maybe they will even make us more productive. Maybe my family and the pugs won't have to move in with my son.

While I'm still the editor, I'd like to welcome Kayla Flanders, senior audit manager at Pella Corp., who joins us as the new contributing editor of "Governance Perspectives." A big thank you to Mark Brinkley for his years serving in that position. And, finally, we will be saying goodbye to InternalAuditor.org's "Marks on Governance" blog at the end of December. Norman Marks' contributions to the magazine have been invaluable. In addition to his blog, he has served as a contributing editor and written numerous articles throughout the years. Norman also was a member of The IIA's Publications Advisory Committee and continues to serve on the magazine's Editorial Advisory Board. We look forward to continued collaborations.

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
OCTOBER 2017
INTERNALAUDITOR.ORG
COSO ERM: It's All About Strategy and Performance
Articulating Materiality
Knowing the Business Inside and Out
Control Self-assessments Address Repeat Findings
This year's Emerging Leaders are ambitious, poised to take on new challenges, and ready to lead.
ON THE RISE
2017

Remove the Emotion

One concept I have introduced to my audit teams is to write the first draft of the audit report with no adjectives or adverbs. After reviewing the facts-based report, we discuss the words that would add color and context. The benefit is twofold. First, it reduces the number of rewrites, and second, it helps the audit team remove the emotion from the audit report without sacrificing the relative importance of the findings.

DENNIS FITZGERALD *comments on Ian Douglas' "Influence, Don't Antagonize" ("In My Opinion," October 2017).*

I agree completely with Ian Douglas. Taking the gentle approach to professionalism is very helpful. People respond better to relationships than merely facts. Yet a balanced approach is needed as people instinctively want to shoot the messenger. We can't help it if clients always want to focus on the negative issues when they are concerned about their jobs. In the end, we cannot ignore who we are, and we need to do our jobs. Whether or not we are friends with the client is not important. What is important is that we protect them in their roles and the organization they represent.

IVETTE REICK *comments on Ian Douglas' "Influence, Don't Antagonize" ("In My Opinion," October 2017).*

Ratings That Work

While I agree in theory with what Jim Pelletier says, practically, management and the audit committee usually look for a comparative yardstick on which to determine the overall level of conformance to a set of standards. Without using some sort of rating scheme, it would be very difficult to provide that yardstick. Even The IIA uses a rating scheme for quality assurance reviews to tell people where they stand.

In my opinion, rating schemes work well if everyone is on board as to what the ratings represent and what the basis for the rating is. If ratings are not defined by the originator and understood by the recipient, people will generally make up their own definition of what the rating means and that's where the issue is. If we as auditors don't provide some sort of "level of concern" to management and the audit committee about what we are reporting, they will draw their own conclusions, which, if significantly different than ours, will undermine what we do.

PAUL FLORA *comments on Jim Pelletier's "From Ratings to Recommendations" ("In My Opinion," August 2017).*

Breaking It Down

I think risk culture and cyber culture are the ones to start with. They are more topical, and expectations around

Ia
INTERNAL AUDITOR
DECEMBER 2017
VOLUME LXXIV:VI

EDITOR IN CHIEF
Anne Millage

MANAGING EDITOR
David Salierno

ASSOCIATE MANAGING EDITOR
Tim McCollum

SENIOR EDITOR
Shannon Steffee

ART DIRECTION
Yacinski Design, LLC

PRODUCTION MANAGER
Gretchen Gorfine

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

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

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

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

PUBLISHED BY THE INSTITUTE OF INTERNAL AUDITORS INC.

CONTACT INFORMATION

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

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

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

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

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

Authorization to photocopy is granted to users registered with the Copyright Clearance Center (CCC) Transactional Reporting Service, provided that the current fee is paid directly to CCC, 222 Rosewood Dr., Danvers, MA 01923 USA; phone: +1-508-750-8400. *Internal Auditor* cannot accept responsibility for claims made by its advertisers, although staff would like to hear from readers who have concerns regarding advertisements that appear.

them are still maturing and being defined. Managers are less likely to feel personally bruised by poor results. They may even want the bad news to drive action on improved culture. Safety is probably the most challenging one, in my opinion.

ROGER NGONG *comments on the Points of View by Pelletier blog post, "Bite-size Culture Audits" (InternalAuditor.org).*

Jurassic Methods

These are all great points in the theoretical world, but in reality it is very difficult to let an auditor simply look for risk and respond. The majority of people require some sort of template, checklist, etc. to work effectively. Unless you are willing to pay for an entire department full of CAE-caliber people, this simply is unrealistic.

Some of the items Chambers mentions as outdated seem to be specifically called for in IIA guidance or desired by management and directors. I would love to do away with this silly audit plan and simply audit based on risk assessments, but, again, it is impractical and hard to prove you have met specific guidelines. Also, in most companies, internal audit has limited time and exposure to directors and executives. Until the norms at the board and audit committee level change to increase their involvement and understanding of internal audit, the Jurassic method will be used because the Jurassic directors and executives prefer it that way.

PAUL *comments on the Chambers on the Profession blog post, "Seven Signs You Might Be a Jurassic Auditor" (InternalAuditor.org).*

Be Forward Looking

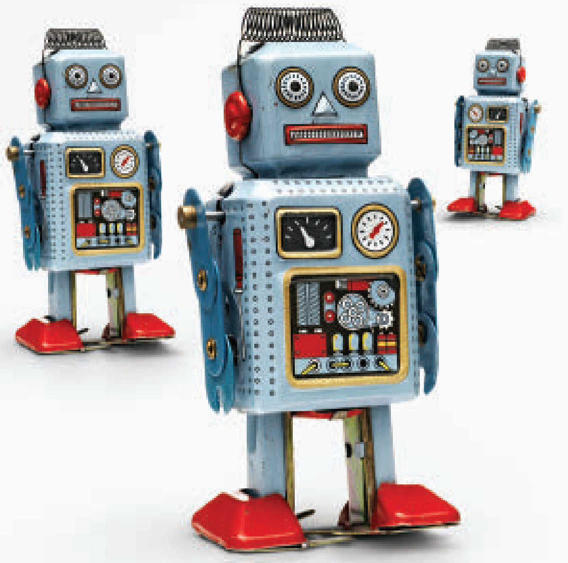
As auditors, we can look at risk management and present a forward-looking review. If we focus on decision-making, we will be reverting to a reactive, backward-facing review. Decision makers often have to make their decisions based on imperfect and incomplete information. To make that an audit finding does not improve the organization and does not inform management. Our current audit focus on achieving objectives and managing risks can do both.

RICK FOWLER *comments on the Marks on Governance blog post, "Maybe Objectives, Risk, and Controls Are the Wrong Focus" (InternalAuditor.org).*

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

S|C
SECURANCE
CONSULTING
OVERCOME YOUR GREATEST RISK.
RISK | SECURITY | COMPLIANCE | PEACE OF MIND
www.SecuranceConsulting.com • 877.578.0215

STATUS QUO IS ONE OF MANY.



Status Go™
IS ONE-ON-ONE.

Ready for an approach that's as
unique as it is personal?

Welcome to Status Go.

gt.com/statusgo

Grant Thornton | Audit | Tax | Advisory

"Grant Thornton" refers to Grant Thornton LLP, the U.S. member firm of Grant Thornton International Ltd (GTIL), and/or refers to the brand under which the independent network of GTIL member firms provide services to their clients, as the context requires. GTIL and each of its member firms are not a worldwide partnership and are not liable for one another's acts or omissions. In the United States, visit grantthornton.com for details. © 2017 Grant Thornton LLP | All rights reserved | U.S. member firm of Grant Thornton International Ltd

Tens of millions pay bribes... Companies lag on social responsibility reporting... Preparing for disaster... NACD recommends heightened cultural oversight.

Update

BOARDS NOT SOLD ON DIVERSITY

Despite investor concerns, directors don't see the value of diversity efforts.

Board members aren't convinced of the importance of racial and gender diversity in the boardroom, according to PwC's 2017 Annual Corporate Directors Survey of 886 U.S. directors. Only 24 percent say racial diversity on the board is very important to bringing diversity of thought to its meetings, while an equal percentage say it is not important at all.

Respondents are somewhat more favorable about gender diversity. More than half (55 percent) say their board needs more gender diversity, and 41 percent say it is very important to developing diversity of thought. Female respondents are more likely to consider gender (68 percent) and racial (42 percent) diversity to be very important, the report notes.

"There's still more work to do on areas such as increasing boardroom diversity, including gender, ethnic, and socioeconomic diversity," says Paula Loop, leader of PwC's Governance Insights Center. Just 21 percent of S&P 500 company board seats are held by women, while among the top 200 S&P companies, racial minorities hold only 15 percent of board seats.

Loop notes that investors are pushing a progressive agenda on diversity, social issues, and shareholder engagement. Indeed,

ARTIFICIAL INTELLIGENCE MAKES AN IMPACT

Security teams say AI gives them an advantage against ransomware and data breaches.

81% say AI detects threats before their security teams.

78% say AI finds threats humans couldn't see.

77% say using AI-powered tools prevents more breaches.

70% say their security team uses AI in its threat prevention strategies.

Source: Cylance, Artificial Intelligence in the Enterprise: The AI Race Is On

IMAGES: TOP, MICHAEL D BROWN / SHUTTERSTOCK.COM; RIGHT, KATEETC / SHUTTERSTOCK.COM

FOR THE LATEST AUDIT-RELATED HEADLINES follow us on Twitter @IaMag_IIA nearly 70 percent of investors responding to a recent Investor Shareholder Services (ISS) global survey view the absence of women on boards as problematic. Forty-three percent say the lack of women directors is indicative of problems in the process for recruiting board members. "Some institutional investors continue to express frustration with a perceived lack of progress in boosting gender diversity in certain markets or industry sectors," ISS states.

Board performance is one area where directors agree with investors—and many don't like what they see, PwC finds. Nearly half of directors say one or more of their colleagues should be replaced.

Boards aren't taking such actions, though. Only 15 percent of respondents say their board has provided an underperforming director counsel or declined to nominate that person for another term. **—T. MCCOLLUM**

66% **OF IT SECURITY PROFESSIONALS ADMIT** they have accessed company information that isn't necessary for their work.

71% **OF IT SECURITY EXECUTIVES** have accessed such information.

45% **HAVE SOUGHT SENSITIVE COMPANY PERFORMANCE INFORMATION.**

"If that information winds up in the wrong hands, corporate data loss, customer data exposure, or compliance violations are possible risks that could result in irreversible damage to the business' reputation or financial standing," says John Milburn, president and general manager of One Identity.

Source: One Identity, annual Global Survey

BRIBERY'S EXTENSIVE REACH

Tens of millions pay bribes across much of the Western Hemisphere.

Nearly 30 percent of Latin American and Caribbean citizens paid a bribe when using key public services such as schools, utility providers, and courts over the last 12 months, according to global anti-corruption watchdog Transparency International (TI). A TI report, People and Corruption: Latin American and the Caribbean, equates this percentage to 90 million individuals in the 20 countries polled.

Despite recent anti-corruption protests across much of the region, almost two-thirds of the 22,000 citizens surveyed say corruption has increased in their country. Only 10 percent say corruption has declined. "Bribery represents a means for enrichment of the few, and a significant barrier to accessing key public services, particularly for the most vulnerable in society," says José Ugaz, TI chair.

Almost half of respondents say most or all police and politicians in their country are corrupt—higher than any other institution. Fifty-three percent say their government is doing a poor job of fighting corruption; 35 percent say it's handled well.

To combat bribery in the region, TI recommends strengthening the rule of law, offering confidential means for citizens to report on their experience with public services, and strengthening institutions that handle corruption-related crimes. **—D. SALIERNO**

THE FINANCIAL RISK OF CLIMATE CHANGE

Companies still lag in reporting on corporate responsibility.

Just 28 percent of large and mid-cap companies globally—and 49 percent of the top 75 U.S. companies by revenue—acknowledge the financial risks of climate change in their annual financial reports, according to KPMG's Survey of Corporate Responsibility Reporting 2017. None of the companies that recognize these risks quantify them in financial terms or use scenario analyses to model the potential financial impact.

"Even among the world's largest companies, very few are providing investors with adequate indications of value at risk from climate change," says Jose Luis Blasco, KPMG's global head of sustainability services.

IMAGES: TOP, ARTGRAPHICS / SHUTTERSTOCK.COM; LEFT, LIGHTSPRING / SHUTTERSTOCK.COM

MORE VISIT www.InternalAuditor.org to read an extended interview with Steven Ulmer.

For the report, KPMG studied 4,900 annual financial reports and corporate social responsibility reports from the top 100 companies by revenue (N100) in 49 countries. The analysis found just five countries where most of the top 100 companies mention climate-related financial risks in their financial reports: Taiwan, France, South Africa, the U.S., and Canada.

Three factors are driving growth in corporate responsibility reporting in annual reports in the U.S., according to Katherine Blue, partner at KPMG's U.S. sustainability services. These are investor and shareholder interest in sustainability, the Securities and Exchange Commission's requirement to include climate change-related disclosures, and the Sustainability Accounting Standards Board's industry-specific Sustainability Accounting Standards advising companies on what should be included in mandatory financial SEC filings.

Globally, the United Nations' Sustainable Development Goals (SDGs), introduced in 2015 to end poverty, protect the planet, and ensure prosperity for all, have made an impact on corporate reporting in the two years since their introduction. Forty-three percent of the largest 250 global companies by revenue are linking corporate responsibility activities to the SDGs, and 39 percent of N100s are doing so. **— S. STEFFEE**

ARE YOU PREPARED?

Recent natural disasters and technology failures demonstrate why disaster recovery should be a part of risk assessments, says Consultant Steven Ulmer.

What is internal audit's role in ensuring the organization has a disaster recovery plan?

As we've recently seen, disasters – whether natural or from human activity – have shown the need for sound disaster recovery plans. Internal auditors play an assurance and consulting role in this arena, so they need to understand attitudes toward disaster recovery risk within their organizations. Disaster recovery should be part of the overall business continuity management process. For organizations that are ad hoc or reactive in their level of disaster recovery maturity, internal audit may need to assist in making the case to senior management for better preparedness.

As part of its risk assessment process, internal audit should examine the plan to determine if operations have been prioritized appropriately, and risk assessments and responses are sufficient and cost effective. Internal audit should note whether the plan is a working document that is updated timely as important changes take place, including acquired businesses and new software and technologies. Based on the level of risk, internal audit should schedule audits of the disaster recovery processes to provide assurance there are no significant gaps.

MAKING CULTURE AN ASSET

The NACD recommends directors heighten their oversight of cultural risks.

A National Association of Corporate Directors (NACD) report calls on boards of directors to apply the same risk oversight to culture as they give to other corporate risks. Directors "need to bring more clarity and rigor to our discussions with management about culture," says Helene Gayle, co-chair of the NACD Blue Ribbon Commission on Culture as a Corporate Asset, which produced the report. Gayle, who is CEO of the McKinsey Social Initiative, says directors need an oversight approach that treats culture as a corporate asset.

The report recommends boards take action in six areas: board oversight responsibilities; boardroom culture assessments; CEO selection and evaluation; reward and recognition systems; shareholder and stakeholder communications; and discussions of strategy, risk, and performance. NACD advises boards to look beyond compliance in setting the scope of their culture oversight. Directors also should get an "on the ground" view by interacting with employees at all organizational levels.

The audit committee can contribute to culture through its oversight of internal and external audit results, employee hotline reports, financial reporting, and risk management processes, the report notes. **— T. MCCOLLUM**

PHOTO: RIGHT, MONKEY BUSINESS IMAGES / SHUTTERSTOCK.COM

BY K.V. HARI PRASAD + EYAD AL RESHAID

EDITED BY JAMES ROTH + WADE CASSELS

INTERNAL AUDIT'S ROLE IN ANTI-MONEY LAUNDERING

Increasing regulatory scrutiny requires auditors to better assess their organization's AML/CFT processes.

The cost of running a compliance function for anti-money laundering and countering the financing of terrorism (AML/CFT) in an organization is far less than the price it may pay for noncompliance. Because of increased regulatory focus, penalties levied affect the bottom line and become a going-concern issue with license suspensions or cancellations. Given the social, economic, and political ramifications of money laundering and terrorism financing, it is becoming more difficult for organizations to consciously ignore AML/CFT compliance. The next 10 years could witness enhanced regulatory compliance across jurisdictions, so internal audit's role in ensuring strict AML/CFT compliance assumes greater importance.

Money laundering is about channeling illegal, "dirty" money through a legitimate means to make it appear as "clean" money within the system. This can be explained in three phases: placement, layering, and integration. In the placement phase, illegal money physically enters into the financial system, such as huge bank account deposits via bank tellers or ATMs. The layering phase involves executing complex transactions with the sole intention of concealing the origin of the funds and diluting the audit trail for further investigations. In the integration phase, the proceeds re-enter the financial system as apparent legitimate funds. Money laundering is a derivative crime; in other words, it is a crime that derives out of another crime. Its nature as a crime depends on the genesis of the funds.

Internal Audit's Role

The money launderer's objective is to convert illegally obtained money into legal tender through inappropriate methods, and in the process avoid the attention of prosecutors or auditors. A clear understanding of AML/CFT helps internal auditors conduct reviews more effectively. At a minimum, internal audit should focus on these areas:

Top management intent. Conduct interviews with key top management individuals. Internal control questionnaires, checklists, and management letters are commonly used in these interviews. However, also assess the willingness and commitment of top management to protect the organization from the threat of money laundering and terrorism financing. This critical exercise should become the basis for review and the depth of sample coverage.

Business operations. Understand the business operations of the organization in detail. Without a

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

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

thorough understanding, auditors will not be able to identify a transaction that is abnormal to the course of business.

Customers. In financial institutions, ensure that the organization is complying with know-your-customer procedures both in form and spirit. Policies and procedures should provide measures for updating know-your-customer forms annually, which establish the identity of the customer, the nature of the customer's activities, and money laundering risks, if any, associated with that customer. Check whether the declarations made by customers in their undertakings are being followed in reality. For example, a customer might declare that he may invest up to $25,000 per year in portfolio management. However, during the year he invests almost $50,000 from undisclosed income. The organization may not raise it as a red flag because of commissions on those transactions.

Risk assessments. Ensure the organization has conducted a risk assessment of customers, geographic affiliations, company products, channels of product routing, etc. Review the nature and volume of transactions and types of products the organization deals with.

Suspicious transactions. By nature, suspicious transactions are more complex and obscure. Internal auditors should get to the bottom of these transactions to ensure they are genuine and should not check them off their list unless they are completely convinced about their purpose. Enhanced due diligence measures should be taken for non-face-to-face business transactions when the customer has not been seen or the business site has not been visited.

Reporting culture. Review the number of suspicious transaction reports raised by the compliance officer during the review period and assess which ones were not reported to the financial intelligent units in the respective countries. These could be false alarms, but scrutinizing those unreported suspicious transactions that could potentially be money laundering transactions may reveal suppression by management and whistleblower silencing.

From and to. All transactions should have the required documentation, including originator and beneficiary details. Missing information in cross-border transactions has caused some of the largest money laundering cases to take a decade or more to resolve, so review all cross-border wire transfers in detail. AML systems also should be reviewed to ensure that the application does not have options to suppress data.

Blacklisted names. Review the AML system and test its capability of capturing data on time, and identifying and red flagging the blacklisted and Specially Designated Persons lists provided by the United Nations and the U.S. Office of Foreign Assets Control, respectively. Determine whether the system is capable of correctly identifying blacklisted names in English and local languages.

Politically exposed persons. People with diplomatic immunity, defined under the politically exposed persons category, are entrusted with a prominent public function and are at higher risk of getting involved in money laundering and terrorism financing transactions. Ensure the organization has mechanisms to identify customers of this category and conducts enhanced due diligence.

Nonprofit organizations. In many countries, organizations with an exempt status become the front-end and most misused vehicles to launder money. Review the grants received, nature and origin of receipts, and ultimate beneficiaries of grants, if it is a recipient organization. In donor organizations, determine whether the donations are made to genuine and reliable nonprofits for a purpose and that those monies are not routed to terrorist networks.

High-risk countries. Engaging with AML/CFT noncompliant countries (assigned as such by the intergovernmental Financial Action Task Force) poses a greater threat for noncompliance. Review how the organization is complying with procedures while dealing with subsidiaries or associates situated in such countries.

Employee protection. Review the whistleblower protection policy and protection to employees raising red flags. Internal sources are many times the strongest lead for an internal auditor in helping detect malpractices in money laundering.

Think Outside the Box

Detecting money laundering and terrorism financing transactions is a challenge for internal auditors because perpetrators bringing ill-gotten money into the system actively conceal the audit trail to avoid prosecution. Because of this, internal auditors conducting AML/CFT reviews should be more vigilant, attentive, and creative to find wrongdoing and ensure compliance. Ia

K.V. HARI PRASAD, CISA, CRISC, *is a partner at Russell Bedford Consulting in Kuwait.*

EYAD AL RESHAID, CIA, CPA, CMA, CISA, *is a senior partner at Russell Bedford Consulting.*

BY JON WEST EDITED BY STEVE MAR

FUNDAMENTALS OF A CYBERSECURITY PROGRAM

Internal auditors and information security professionals can join forces to prepare the organization for cyber threats.

Recent major data breaches at Equifax and Deloitte are reminders of the dangers of failing to practice cybersecurity fundamentals. At Equifax, more than 143 million records were exposed, including names, addresses, Social Security numbers, and credit information. The Deloitte breach compromised hundreds of global clients' information.

Cybersecurity risk is not just an IT issue—it's a business and audit issue. Collectively, the advice information security and internal audit professionals provide to business leaders has never been more important. To partner in addressing today's cybersecurity challenges, audit and security leaders must start with a little common sense.

Take, for example, a homeowner. There are valuables in the home, so it's important that only trusted people have a copy of the house key. To be prudent, the homeowner should take an inventory of the items in the home and estimate their value so he or she knows how much needs protecting and ensures items are stored securely. The homeowner also should make sure the smoke detectors are working and set up a security monitoring service with video surveillance so he or she can be alerted and react quickly to a potential fire or break-in.

Organizations need to exercise the same principles when assessing the digital risk to customer, employee, and other company information. Auditors and security professionals should prioritize three fundamentals to help make an information security program more impactful and effective.

1. Improve Visibility

How can organizations protect what they can't see? Identifying the valuables, or assets, within an organization is probably the most foundational aspect of a security program, and yet it continues to be a pain point. Technical solutions can help, with the right support and funding, but asset management is a process and a discipline, not just a tool.

Knowing the organization's assets and their value will inform what gets monitored and how. Security monitoring solutions are improving, with richer analytics and machine-learning capabilities as well as more expansive integration. Organizations should monitor their environments around the clock. For small and mid-size organizations that lack in-house resources for such monitoring, partnering with a trusted third party or managed security service provider is an option.

Another fundamental aspect of improving visibility and monitoring is to proactively look for existing weaknesses or vulnerabilities

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

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

and patch them. Failure to patch systems with the Apache Struts vulnerability led to the Equifax data breach. The vulnerability allows command injection attacks to occur because of incorrect exception handling. As a result, an unauthorized user can gain privileged user access to a web server and execute remote commands against it. This vulnerability could have been addressed by standardizing and increasing the frequency of scanning and patch cycles.

Security and audit teams can work together to ensure the right risks are being mitigated and help their business partners think about risk rather than checking off a compliance requirement. They also can partner on implementing a repeatable risk assessment process. This is no longer just a best practice or standard. It is now a matter of compliance with regulations such as the European Union General Data Protection Regulation and the New York Department of Financial Services CR500.

2. Improve Resiliency

Is the organization prepared to handle the inevitable and how well can it recover? Improving visibility and being notified of threats and incidents is great, but an inappropriate or untimely response can incur a much greater cost. The organization's ability to quickly diagnose, contain, and recover from a potential or actual data breach or privacy incident directly impacts business operations and the cost to the organization. A well-planned and tested incident response plan can reduce the overall impact and cost of the incident.

Maintaining a state of preparedness is more than periodically testing the plan.

Rapid response is a must with many global and U.S. state data breach notification laws having aggressive notification time lines. One of the ways in which internal audit and information security functions can increase the speed of their investigations and response times is maintaining a good asset-management process.

Maintaining a state of preparedness is more than having a document or periodically testing the plan. It's about having a good team of people from the right areas of the organization. Security and audit teams can partner to ensure that the incident response plan has all the necessary elements in place and ensure it is being followed. Responding to a crisis requires people to work together in a way that they normally do not work, which requires building and maintaining good relationships.

3. Improve Sensitivity

Do the organization's employees and associates understand what is at stake with cybersecurity? Increasing sensitivity to cyber risks needs to be tied to personal relevance, because people respond better when it impacts them directly.

Recall the homeowner analogy. For some people, it may be easy to get too comfortable within their neighborhood and become desensitized to potential risks of home thefts to the point of forgetting to lock doors and windows. Or they may become too liberal about who has a copy of their house key and what they do with it. There are lessons here for employees that should prompt their response.

Social engineering, including phishing simulations and physical security, must be a regular and primary aspect of cyber risk sensitivity training programs. Phishing attacks aimed at stealing user login credentials cause most reported data breaches. These types of attacks can be thwarted through a more expansive use of multi-factor authentication, which is a combination of something the person knows, such as a password or PIN number, along with something the person has, such as a token or smartphone. Technical controls can be effective, but they also must be accompanied by user education. As a training method, phishing simulations confirm what internal auditors and security professionals already know: There is never going to be a 0 percent click rate. However, they provide an opportunity to reiterate training content.

Practicing Security Basics

Shortly after the 2014 Sony hack, former President Barack Obama compared cybersecurity to a basketball game, "in the sense that there's no clear line between offense and defense. Things are going back and forth all the time." There is some truth to that.

In basketball, teams often lose because they overreact to a new play and forget the fundamentals. Coaches usually react by having teams practice basics such as passing, layups, and free throws. Similarly, organizations all have various priorities, and many of them are competing. Sometimes when it appears organizations are getting beaten by cyber risks, they need to revisit the fundamentals such as visibility, resiliency, and sensitivity. Auditors can partner with chief information security officers in this effort to ensure that the program is taking a balanced, risk-based, and business-oriented approach. ia

JON WEST, CISM, CISSP, CIPT, PCIP, *is chief information security officer at Kemper Corp. in Jacksonville, Fla.*

Risk Watch

BY CHARLIE WRIGHT

TOMORROW'S ERM TODAY

Disruptive technology risks are becoming a critical concern for internal auditors.

As enterprise risk management (ERM) programs continue to mature at organizations around the world, internal auditors are now facing a new challenge. Technology risks are evolving and changing so rapidly, it is difficult for management to assess the new threats and adjust its strategies to manage and mitigate them. Applications that use disruptive technologies, such as artificial intelligence, advanced robotics, 3D printing, blockchain, and the Internet of Things, are being designed quickly and often generate new high-growth markets. Internal auditors are struggling to stay abreast of the most recent developments and identify new internal controls that add value.

Additionally, the exponential growth of computing power has enabled organizations to capitalize on the use of mobile devices and leverage the ubiquity of the internet to reach their markets almost instantly. While this is an exciting and challenging opportunity for marketers and business managers, it has injected new risk considerations for internal auditors.

Business Advances

Digitalization of data has created opportunities to improve data analytics, use algorithms to facilitate cognitive intelligence, and create bot applications that perform automated tasks. The essence of the risks and controls has not changed as much as the underlying technology. The processes still need to adhere to organizational policies and procedures, change management practices are still a vital component in transitioning to new tools and processes, and system and access controls must be enforced.

However, some controls that were important in the past now take on a new level of criticality. Automated algorithms result in less transparency of the underlying process. When data is used and shared through these processes, accuracy, and completeness become a necessity. An organization needs very specific controls to ensure a bot does not proliferate erroneous data. Information security and access control processes must treat the bot as if it were a person and only allow access to appropriate data. Checks and balances must be integrated into the process to ensure the results are accurate, service level agreements are met, and contracts are adhered to.

Advanced materials, 3D printing, and autonomous vehicles are other advances that are transforming the business landscape. New businesses created by these technologies need to follow established governance processes and design risk management and internal controls into their business processes. As entirely new markets and products are developed, it is important that risk managers and internal auditors are involved proactively.

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

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

Many applications using the cloud and the internet are being transformed by another new underlying process called blockchain. Blockchain is a distributed ledger that maintains a shared list of records. Each of these records contains time-stamped data that is encoded and linked to every other previous transaction in that chain of transactions. The decentralized and distributed storage of these records provides visibility to everyone in the network and ensures that no single entity can change any of the historical records. While blockchain is already being used in numerous applications, most notably digital currencies, many other industries are exploring the technology. Banks are testing cross-border financial transactions, and there is much speculation about the potential to use blockchain to eliminate the middle man in real estate deals, contracts, stock purchases, and other similar transactions. If blockchain is effective at eliminating intermediaries, the new business model will expose all the transacting parties to new risks, which were previously being managed by the middle man.

Audit's Effect on Disruption

There are several ways internal auditors can help manage the effect of disruptive technologies on their organizations. By focusing on assurance, providing insight to management, and demonstrating proficiency and expertise in new technologies, internal auditors will be able to contribute significantly to the overall success of their organizations.

> **Internal auditors must constantly pursue training on new technologies.**

Focus on Assurance For many years organizations have been encouraged to focus on what they do best. That is wise advice for the internal audit profession, as well. By continuing to focus on governance, risk, and internal controls, auditors can help ensure processes are designed and operating effectively. Regardless of the nature or tempo of the changes, auditors will then be able to fulfill their mission. Moreover, proactively helping their organizations anticipate emerging risks and technological changes can position internal audit as an authority and help prepare the organization to respond to disruptive events.

Engage With Stakeholders and Subject-matter Experts By aligning with the expectations of its key stakeholders and working closely with subject-matter experts who are implementing disruptive technologies, internal audit can be focused on the most relevant and significant issues. For example, cybersecurity and data privacy are topics that every organization is managing. Identifying trends that will affect the organization, and collaborating with and providing insight to their stakeholders, can enable internal audit to significantly affect the business agenda.

Invest in Training on Disruptive Technologies More than ever, internal auditors must constantly pursue training to learn about new technologies and the complex and emerging new risks being introduced into their organizations. Additionally, chief audit executives need to focus on developing an adaptive, flexible, innovative staffing model. This new model must tap into a highly specialized talent pool that has the technological competence to rapidly understand and leverage new tools, techniques, and processes.

Put New Technologies to Work Perhaps the most important thing auditors can do to prepare for technological innovations is to embrace and leverage new technologies in their own work. Internal auditors need to be at the forefront of adopting artificial intelligence, cognitive computing, and smart robots. Auditors need to completely understand how technologies like blockchain work and how they can be used in their organizations. They must take advantage of machine learning and data analytics in their audit processes. Moreover, continuous auditing should be the standard default for new audit routines, and real-time auditing should be a requirement as organizations implement new business processes.

An Audit Upgrade

Just when organizations were getting a handle on ERM, the threat of disruptive technologies has arrived and will affect every organization regardless of its size or objectives. When Gordon Moore observed in 1965 that the number of transistors on an integrated circuit had doubled every year since transistors were invented, one doubts he imagined that exponential growth would continue for more than 50 years. As computing power increases, technology becomes more mobile, data becomes more accessible and usable, and new competitors capitalize on the opportunities that arise. Risk managers will have to assess emerging threats consistently. Internal auditors will need to respond to those threats with new and better ways to perform audits and redesign their own processes—or they may face disruption, themselves.

CHARLIE WRIGHT, CIA, CISA, CPA, *is director, Enterprise Risk Solutions, at BKD LLP in Edmond, Okla.*

AUDITOR SPOTLIGHT

CARLO P. CASAGRANDE, CISA, CRISC, CFE

As a director in Nielsen's Internal Audit department, Carlo Casagrande works at the forefront of the highly competitive and rapidly changing environment that is digital audience measurement. In addition to directing risk assessments and internal audits, Carlo also serves as Nielsen's digital measurement compliance leader, helping to align Nielsen with digital ratings industry standards, guidelines and best practices.

We asked Carlo to share insights from his current role and career path.

Q: You have a diverse background in audit and media measurement. Can you share how you arrived in your current role?

A: I came to Nielsen from EY, where I was an external auditor of data ratings services seeking compliance with industry regulations. I worked with a variety of measurement vendors, ad servers and publishers across digital, television, audio and mobile platforms to provide audit opinions on the effectiveness of internal controls, IT general controls and compliance with third-party standards.

I have a bachelor's degree in accounting, and prior to joining EY, I worked as a tax auditor for the State of Florida. I was also an internal auditor for a global financial services firm before that, so I have been doing audit in some form – whether it be internal or external, financial, operational, compliance, IT, etc. – for more than 10 years, and each of these roles has brought with it a distinct perspective on similar issues.

Carlo maintains the Certified Information Systems Auditor (CISA), Certified in Risk and Information Systems Control (CRISC) and Certified Fraud Examiner (CFE) professional designations. He also recently passed the certificate programs for the COSO Internal Controls Certificate offered by the IIA and the Cybersecurity Nexus Fundamentals (CSX-F) from ISACA.

Q: You have numerous certifications. What would you advise to others who are considering investing in training for professional certifications?

A: It's a good idea to spend time thinking about your training and certification path carefully. Talk to your leaders to understand where they want to grow the team's collective skill set, so you know the certifications you pursue will also bring value to your organization.

For some, obtaining a certification can immediately impact their career by qualifying them for a promotion, as the CISA did for me when preparing to become a manager. But, it can also be used to expand your knowledge base and drive your career in a new direction. This is especially important in today's job market, where advancements in technology are creating new skill sets and quickly causing others to become obsolete, or at least less relevant.

Continuing education demonstrates to your employer and your clients that you are dedicated to ongoing excellence, and shows that you are up to date with the best practices in your field.

Q: Media consumption has been heavily disrupted in the past decade. What are the challenges of being an internal auditor in an industry where the pace of change is so rapid?

A: The greatest risks today in the media measurement and rating industry are the constant advances in technology and rapidly shifting environment. Not only are the demands of technology heightening in complexity, but consumer behaviors are becoming more volatile, making it difficult to predict what clients will desire in the near future. We, as auditors in this field, need to be growing and adapting as rapidly as the environment itself if we want to continue to deliver value to our organizations.

Security is also critical to every organization's success, as we have all seen in the high-profile breaches that have been in the news just this year. This is one reason I have chosen to focus my recent continuing education efforts around risk management and cybersecurity. These fields are growing for a reason. The risks posed to information security threaten companies' reputations, profitability and their very existence.

nielsen

BY SCOTT MARK EDITED BY BRYANT RICHARDS

STEALING WELLNESS

Detecting drug diversion fraud within hospitals is a collaborative process.

While attending a conference, Angus Munro, the CEO of a large academic medical center, heard from colleagues about their experiences with drug diversion, something he was increasingly concerned about within his hospital. Drugs represented almost 20 percent of his costs and were increasing annually. Conversations with his director of pharmacy left him unsatisfied with the rigor of controls in place for these multimillion-dollar inventory stores. While his primary concern was centered on the exceptionally expensive noncontrolled drugs, he also was aware of the growing opioid abuse problem in the community. If a newspaper story implicated the hospital in contributing to the crisis through poor internal controls, it would be devastating. He immediately contacted Mary Nicholls, the chief audit executive (CAE), to test internal controls.

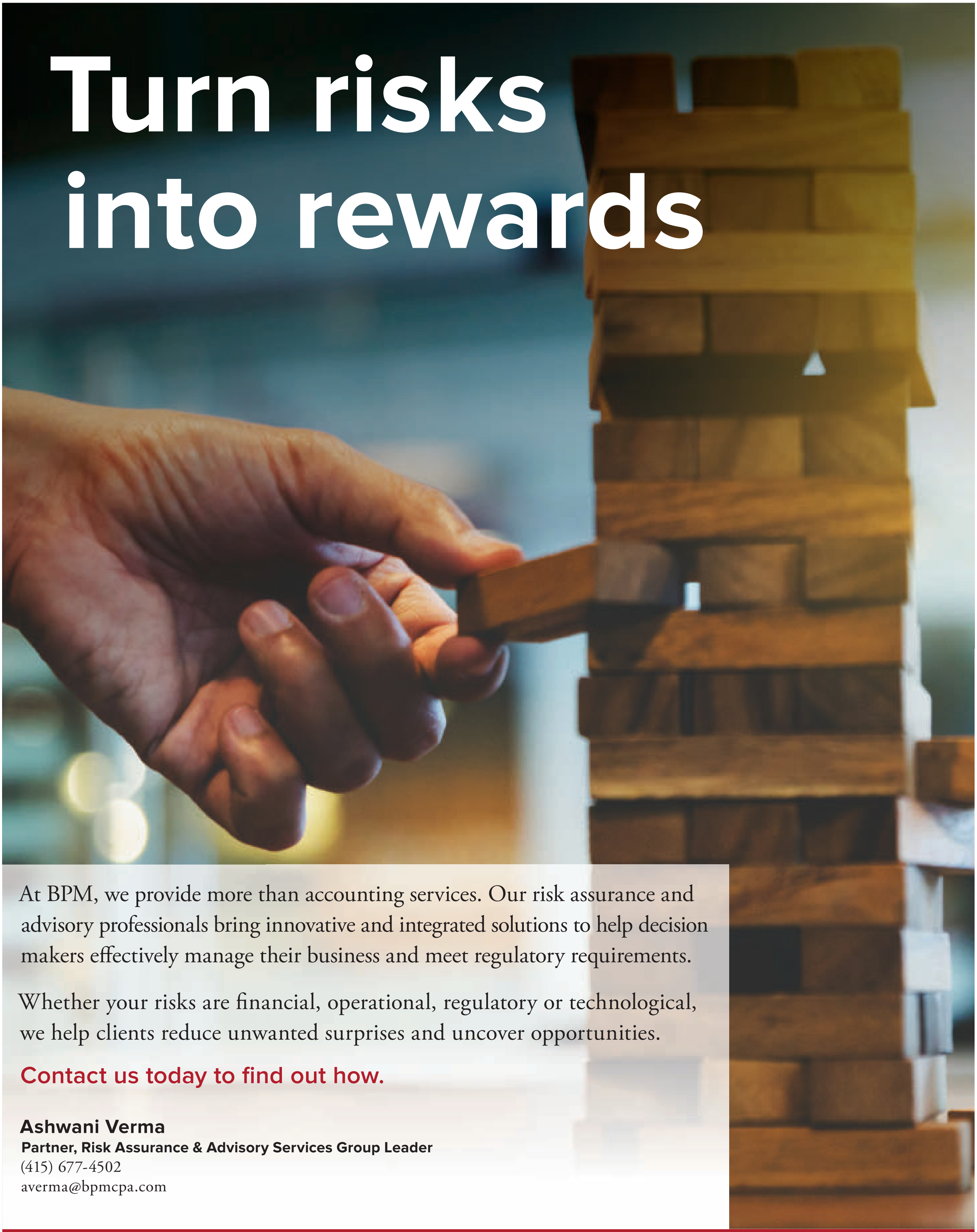
After some research, Nicholls learned that pharmaceutical diversion was on the rise nationally, and the methods had become more sophisticated. Recent diversion rings involved multiple hospitals and several actors actively collaborating at numerous levels of the organization. Historically, prescription drug diversion from pharmacies almost exclusively involved controlled substances (narcotics and other commonly abused drugs), primarily schedule II narcotics and other opioids that have a high potential for abuse and dependence. These medications were sold on the street directly to addicted individuals.

Also contributing to diversion was the emergence of "pill parties" and "rave parties." These were common among middle and high school students who raided their parents' medicine cabinets or worked in areas to obtain access to random medications for party guests.

Even more troubling to Nicholls were reports of amateur chemists making illegal drugs using noncontrolled prescription drugs and over-the-counter (OTC) drugs. For example, the commonly used OTC cold medication pseudoephedrine can be used to make methamphetamine or crystal meth. Because of this, some OTC medications became available only via prescription, and some prescription drugs were made controlled. Nicholls concluded that there was sufficient risk to perform a rigorous audit of controls around medication use.

While Nicholls knew she may not detect any active diversion, she also knew that people often compromise their ethics out of necessity during times of distress, uncertainty, and economic hardship. Many healthcare insurance plans do not cover new, high-cost biologic, HIV, and chemotherapy medications. This, combined with loss of employment,

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



Turn risks into rewards

At BPM, we provide more than accounting services. Our risk assurance and advisory professionals bring innovative and integrated solutions to help decision makers effectively manage their business and meet regulatory requirements.

Whether your risks are financial, operational, regulatory or technological, we help clients reduce unwanted surprises and uncover opportunities.

Contact us today to find out how.

Ashwani Verma
Partner, Risk Assurance & Advisory Services Group Leader
(415) 677-4502
averma@bpmcpa.com

bpmcpa.com/RAAS

BPM

TAX I ASSURANCE I ADVISORY

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

LESSONS LEARNED

- » While professional practices in health care may not traditionally control medications that have low abuse potential, the risk and inventory controls still need to be placed on high-cost items.
- » CAEs and risk managers play a key role in assuring that hospitals and health systems comply with audit and control standards, regardless of traditional professional practices.
- » Health-care professional practices need to be rigorously tested against audit and compliance standards to evaluate risk and vulnerabilities.
- » Health-care professionals rarely review operational practices through an audit, compliance, and accounting lens, and benefit greatly from the expertise of a CAE.
- » Pharmaceutical drugs represent an average of 20 percent of hospital costs, and failure to control their diversion can have a material impact on financial statements.
- » Poor medication control can lead to medication diversion and represents a significant risk to hospital reputations when reported in the media.

has resulted in the emergence of a black market for high-cost, noncontrolled pharmaceuticals. In these cases, the patrons are not addicted individuals, but rather sick patients or family members who are unable to afford their medications.

The largest diversion ring discovered in the U.S. began with a pharmacy inventory employee stealing a noncontrolled bone marrow drug for a relative with cancer who was unable to pay for it. The employee soon discovered a black market for patients in need and recruited other employees within his hospital and surrounding hospitals.

Ironically, the discovery was made when the truck carrying the diverted drugs was hijacked by thieves expecting to steal pharmaceutical-grade narcotics. The hijackers deserted the truck when they discovered it was filled with HIV, cancer, and biologic medications. The hijackers were caught, which led police to the diversion ring. Eventually, it was discovered that some of the stolen medications were being sold back to the wholesalers for redistribution to the same hospitals.

Within her hospital, Nicholls found that controlled substances had stronger controls (automation, double counts and checks, and segregations of duties) than noncontrolled substances, which can cost tens of thousands of dollars per dose. In the pharmacy, she found that there was one person assigned to create purchase orders (POs), place orders, receive medications, and reconcile orders to POs. The lack of segregation of duties demonstrated a significant opportunity for diversion. Nicholls also learned that due to the unique nature of medication-use oversight, the pharmacy was exempt from the safeguards that were in place within the materials management department and other areas of supply chain oversight.

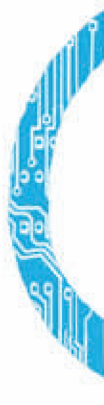
An audit of the purchasing records found high-cost chemotherapy medications and other drugs that were no longer in inventory and for which dispensing records did not support their use in patient care. A select audit of the two highest-cost drugs against their recorded use showed significant discrepancies, suggesting a material and pervasive problem that approximated 20 percent of purchases.

Within the pharmacy, noncontrolled medications are generally stored on open shelves and in unlocked refrigerators because of the mindset that only drugs of abuse would be targeted for theft. Inventories were only taken annually, but not reconciled against purchases, usage, or waste. As a result, it was not possible to determine shrinkage by theft or other causes. In addition, hospital computer systems are not designed to reconcile medications administered with hospital purchases, as one might reconcile sales to purchases in a retail operation.

Nicholls quickly concluded that insufficient levels of controls for pharmacy and medication-use systems, combined with the high street value of these medications, provided a significant opportunity for a diversion ring within the hospital. She recommended a comprehensive audit to scope the material impact on the hospital's financial statements.

Furthermore, any diverted medications could create a potential source of litigation for the hospital. Background research revealed several high-profile medication diversion rings around the country at medical institutions such as the University of Colorado, the University of Maryland, and Georgetown University, which resulted in fines, jail time, and public embarrassment. The settlement in the case at Georgetown University Hospital resulted in the sale of the hospital by the university to settle the claims. Here, the diverters replaced unused medications with used vials, exposing patients to infectious diseases. The judgment in the class-action lawsuit exceeded the ability of the hospital to pay the claim. Ia

SCOTT MARK, PHARMD, *is vice president at Craneware Healthcare Intelligence in Pittsburgh.*



audit in an age of intelligent machines

Tim McCollum

Illustration by Mick Wiggins

Already in use at many organizations, artificial intelligence is poised to transform the way business operates.

While monitoring transactions, an alert bank data analyst noticed unusual payments from a computer manufacturer to a casino. Because casinos are heavily computerized, one would expect the payments to go to the computer company. The analyst alerted an investigative agent, who rapidly scoured websites, proprietary data stores, and dark web sources to find detailed information about the two parties. The data revealed that the computer manufacturer was facing a criminal indictment and a civil law suit. Meanwhile, the casino had lost its gambling license due to money laundering and had set up shop in another country. Further investigation revealed the computer manufacturer was using the casino to launder money before the company's legal issues drove it out of business.

The bank's data analyst was a machine learning algorithm. The investigative agent was an artificial intelligence (AI) agent.

AI is all around. It's monitoring financial transactions. It's diagnosing illnesses, often more accurately than doctors. It's carrying out stock trades, screening job applicants, recommending products and services, and telling people what to watch on TV. It's in their phones and soon it will be driving their cars.

And it's coming to organizations, maybe sooner than people realize. Research firm International Data Corp. says worldwide spending on cognitive and AI systems will be $12 billion this year. It predicts spending will top $57 billion by 2021.

"If you think AI is not coming your way, it's probably coming sooner than you think it is," says Yulia Gurman, director of internal audit and corporate

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

“Internal auditors should be alerting the board about what’s coming their way.”

Yulia Gurman

“The technology is never going to accuse somebody of a crime or a regulatory violation.”

David McLaughlin

security for the Packaging Corporation of America in Lake Forest, Ill. Fresh off of attending a chief audit executive roundtable about AI, Gurman says AI wouldn’t have been on the agenda a year ago. Like most of her peers present, she hasn’t had to address AI within her organization yet. Now it’s on her risk assessment radar. “Internal auditors should be alerting the board about what’s coming their way,” she says.

THE LEARNING ALGORITHM

Intelligent technology has already found a place on everyday devices. That personal assistant on the kitchen counter or on the phone is an AI. Alexa, Cortana, and Siri can find all sorts of information for people, and they can talk to other machines such as alarm systems, climate control, and cleaning robots.

Yet, most people don’t realize they are interacting with AI. Nearly two-thirds of respondents to a recent survey by software company Pegasystems say they have not or aren’t sure they have interacted with AI. But questions about the technologies they use—such as personal assistants, email spam filters, predictive search terms, recommended news on Facebook, and online shopping recommendations—reveal that 84 percent are interacting with AI, according to the What Consumers Really Think About AI report.

What makes AI possible is today’s massive availability of data and computing power, as well as significant advances in the quality of the machine learning algorithms that make AI applications possible, says Pedro Domingos, a professor of computer science at the University of Washington in Seattle and author of *The Master Algorithm*. When AI researchers like Domingos talk about the technology, they often are referring to machine learning. Unlike other computer applications that must be written step-by-step by people, machine learning algorithms are designed to program themselves. The algorithm does this by analyzing huge amounts of data, learning about that data, and building a predictive model based on what it’s learned. For example, the algorithm can build a model to predict the risk that a person will default on his or her credit card based on various factors about the individual, as well as historical factors that lead to default.

DRIVEN BY DATA

Using AI to make predictions takes huge amounts of data. But data isn’t just the fuel for AI, it’s also the killer application. In recent years, organizations have been trying to harness the power of big data. The problem is there’s too much data for people and existing data mining tools to analyze quickly.

That is among the reasons why data-driven businesses are turning to AI. Five industries—banking, retail, discrete manufacturing, health care, and process manufacturing—will each spend more than $1 billion on AI this year and are forecast to account for nearly 55 percent of worldwide AI spending by 2021, according to IDC’s latest Worldwide Semiannual Cognitive Artificial Intelligence Systems Spending Guide. What these industries have in common is lots of good data, says David Schubmehl, research director, Cognitive/AI Systems, at IDC. “If you don’t have the data, you can’t build an AI application,” he explains. “Owning the right kind of data is what makes these uses possible.”

Retail and financial services are leading the way with AI. In retail, Amazon’s AI-based product recommendation solutions have pushed other traditional and online retailers like Macy’s and Wal-Mart Stores Inc. to follow suit. But it’s not just the retailers themselves that are driving product recommendations, Schubmehl says. Image recognition AI

Artificial intelligence will add **$15.7 trillion** to the global **economy** by **2030**, led by China and North America, PwC's AI Sizing the Prize study reports.

apps can enable people to take a picture of a product they saw on Facebook or Pinterest and search for that product—or something similar and less expensive. "It's a huge opportunity in the marketplace," he says.

Meanwhile, banks and financial service firms are using AI for customer care and recommendation systems for financial advice and products. Fraud investigation is a big focus. "The idea of using machine learning and deep learning to connect the dots is something that is very helpful to organizations that have traditionally relied on experienced investigators to have that 'aha moment,'" Schubmehl says.

That's what happened with the casino and the computer manufacturer. "The way AI works in that scenario is to say, 'Something is different. Let's bring it back to the central brain and analyze whether this is risky or not risky,'" says David McLaughlin, CEO and founder of AI software company QuantaVerse, based in Wayne, Pa. "The technology is never going to accuse somebody of a crime or a regulatory violation. What it's going to do is allow the people who need to make that determination focus in the right areas."

Currently, IDC says automated customer service agents and healthcare diagnostic and treatment systems are the applications where organizations are investing the most. Some of the AI uses expected to rise the most over the next few years are intelligent processing automation, expert shopping advisors, and public safety and emergency response.

Regardless of the use, Schubmehl says it's the business units that are pushing organizations to adopt AI to advance their business and deal with potential disrupters. Because of the computing power needed, most industries are turning to cloud vendors, some of whom may also be able to help build machine learning algorithms.

THE JOBS QUESTION

By now, internal auditors may be asking themselves, "Is AI going to take my job?" After all, an Oxford University study rated accountants and auditors among the professionals most vulnerable to automation. Of course, internal auditors aren't accountants. But are their jobs safe?

Actually, AI may be an opportunity, says IDC's David Schubmehl. He says many of the manual processes internal auditors review are going to be automated. Auditors will need to check how machine learning algorithms are derived and validate the data on which they are based. And, they'll need to help senior executives understand AI-related risks. "There's going to be tremendous growth in AI-based auditing, looking at risk and bias, looking at data," Schubmehl explains. "Auditors will help identify and certify that machine learning and AI applications are being fair."

Using AI to automate business processes will create new risks for auditors to address, says Deloitte & Touche LLP's Will Bible. He likens it to when organizations began to deploy enterprise resource planning systems, which shifted some auditors' focus from reviewing documents to auditing system controls. "I don't foresee an end to the audit profession because of AI," he says. "But as digital transformation occurs, I see the audit profession re-evaluating the risks that are relevant to the audit."

IS AI SOMETHING TO FEAR?

Despite its potential, there is much fear about the risks that AI poses to both businesses and society at large. Some worry that machines will become too smart or get out of control.

There have been some well-publicized problems. Microsoft developed an AI chatbot, Clippy, that after interacting with people, started using insulting and racist language and had to be shut down. More recently, Facebook shut down an experimental AI system after its chatbots started communicating with each other in their own language, in violation of their programming. In the financial sector, two recent stock market "flash crashes" were attributed to AI applications with unintended consequences.

Respondents to the World Economic Forum's (WEF's) 2017 Global Risks Perception Survey rated AI highest in potential negative consequences among 12 emerging technologies. Specifically, AI ranked highest among technologies in economic, geopolitical, and technological risk, and ranked third in societal risk, according to the WEF's Global Risks Report 2017.

Employment One of the biggest concerns is whether AI might eliminate many jobs and what that might mean to people both economically and personally. Take truck driving, the world's most common profession. More than 3 million people in the U.S. earn their living driving trucks and vans. Consulting firm McKinsey predicts that one-third of commercial trucks will be replaced by self-driving vehicles by 2025.

According to the Pew Research Center's recent U.S.-based Automation in Everyday Life survey, 72 percent of respondents are worried about robots doing human jobs. But only 30 percent think their own job could be replaced (see "The Jobs Question"

To learn more about internal audit's role in AI, DOWNLOAD The IIA's Artificial Intelligence: Considerations for the Profession of Internal Auditing.

on page 27). That may be wishful thinking. "However long it takes, there's not going to be any vertical industry where there's not the opportunity to automate humans out of a job," says John C. Havens, executive director of the IEEE Global AI Ethics Initiative. He says that will be the case as long as businesses are measured primarily by their ability to meet financial targets. "The bigger question is not AI. It's economics."

Ethics With organizations racing to develop AI, there is concern that human values will be lost along the way. Havens and the IEEE AI Ethics Initiative are advocating for putting applied ethics at the front end of AI development work. Consider the emotional factors of children or elderly persons who come to think of a companion robot in the same way they would a person or animal. And who would be accountable in an accident involving a self-driving car—the vehicle or the person riding in it?

"The phrase we use is 'ethics is the new green,'" Havens explains, likening AI ethics to the corporate responsibility world. "When you address these very human aspects of emotion and agency early on—much earlier than they are addressed now—then you build systems that are more aligned to people's values. You avoid negative unintended consequences and you identify more positive opportunities for innovation."

Privacy and Security Using AI to gather data poses privacy risks for both individuals and businesses. All those personal assistant requests, product recommendations, and customer service interactions are gathering data on people—data that organizations eventually could use to build a comprehensive model about their customers. Organizations using personalization agents must walk a fine line. "You want to personalize something to the point where you can get the purchase offer," Schubmehl says, "but you don't want to personalize it so much that they say, 'This is really creepy and knows stuff about me that I don't want it to know.'"

All that data creates a compliance obligation for organizations, as well. And it is also valuable to cyber attackers.

Output Although AI has potential to help organizations make decisions more quickly, organizations need to determine whether they can trust the AI model's recommendations and predictions. That all depends on the reliability of the data, Domingos says. If the data isn't reliable or it's biased, then the model won't be reliable either. Moreover, machine learning algorithms can overinterpret data or interpret it incorrectly. "They can show patterns," he points out. "But there are other patterns that would do equally well at explaining what you are seeing."

Control If machine learning algorithms become too smart, can they be controlled? Domingos says there are ways to control machine learning algorithms, most notably by raising or lowering their ability to fit the data such as through limiting the amount of computation, using statistical significance tests, and penalizing the complexity of the model.

He says one big misconception about AI is that algorithms are smarter than they actually are. "Machine learning systems are not very smart when they are making important decisions," he says. Because they lack common sense, they can make mistakes that people can't make. And it's difficult to know from looking at the model where the potential for error is. His solution is making algorithms more transparent and making them smarter. "The risk is not from malevolence. It's from incompetence," he says. "To reduce the risk from AI, what we need to do is make the computer smarter. The big risk is dumb computers doing dumb things."

Internal audit could use AI to analyze an entire data set to identify cases that require the most scrutiny.

Knowledge Domingos says concerns about AI's competence apply as well to the people who are charged with putting it to use in businesses. He sees a large knowledge gap between academic researchers working on developing AI and the business employees building machine learning algorithms, who may not understand what it is they are doing. And he says, "Part of the problem is their bosses don't understand it either."

Governance That concern for governance is one area the WEF's Global Risk Report questions—specifically, whether AI can be governed or regulated. Components of AI fall under various standards bodies: industrial robots by ISO standards, domestic robotics by product certification regulations, and in some cases the data used for machine learning by data governance and privacy regulations. On their own, those pieces may not be a big risk, but collectively they could

VISIT InternalAuditor.org to learn more about how organizations are putting AI to use, including applications for gathering customer information.

be a problem. "It would be difficult to regulate such things before they happen," the report notes, "and any unforeseeable consequences or control issues may be beyond governance once they occur."

AI IN IA

Questions of risk, governance, and control are where internal auditors come into the picture. There are similarities between deploying AI and implementing other software and technology, with similar risks, notes Will Bible, audit and assurance partner with Deloitte & Touche LLP in Parsippany, N.J. "The important thing to remember is that AI is still computer software, no matter what we call it," he says. One area where internal auditors could be useful, Bible says, is assessing controls around the AI algorithms—specifically whether people are making sure the machine is operating correctly.

If internal auditors are just getting started with AI, their external audit peers at the Big 4 firms are already putting it to work as an audit tool. Bible and his Deloitte colleagues are using optical character recognition technology called Argus to digitize documents and convert them to a readable form for analysis. This enables auditors to use data extraction routines to locate data from a large population of documents that is relevant to the audit.

For auditors, AI speeds the process of getting to a decision point and improves the quality of the work because it makes fewer mistakes in data extraction. "You can imagine a day when you push a button and you're given the things you need to follow up on," Bible says. "There's still that interrogation and investigation, but you get to that faster, which makes it a better experience for audit clients."

"You don't want to personalize it so much that they say, 'This is really creepy and knows stuff about me that I don't want it to know.'"

David Schubmehl

"Part of the problem is their bosses don't understand [AI] either."

Pedro Domingos

QuantaVerse's McLaughlin says internal auditors could take AI even farther by applying it to areas such as fraud investigation and compliance work. For example, rather than relying on auditors or compliance personnel to catch potential anti-bribery violations, internal audit could use AI to analyze an entire data set of expense reports to identify cases of anomalous behavior that require the most scrutiny. "Now internal audit has the five cases that really need a human to understand and investigate," McLaughlin says. "That dramatically changes the effectiveness of an internal audit department to protect the organization."

The key there is making sure a person is still in the loop, Bible says. "The nature of AI systems is you are throwing them into situations they probably have not seen yet," he notes. A person involved in the process can evaluate the output and correct the machine when it is wrong.

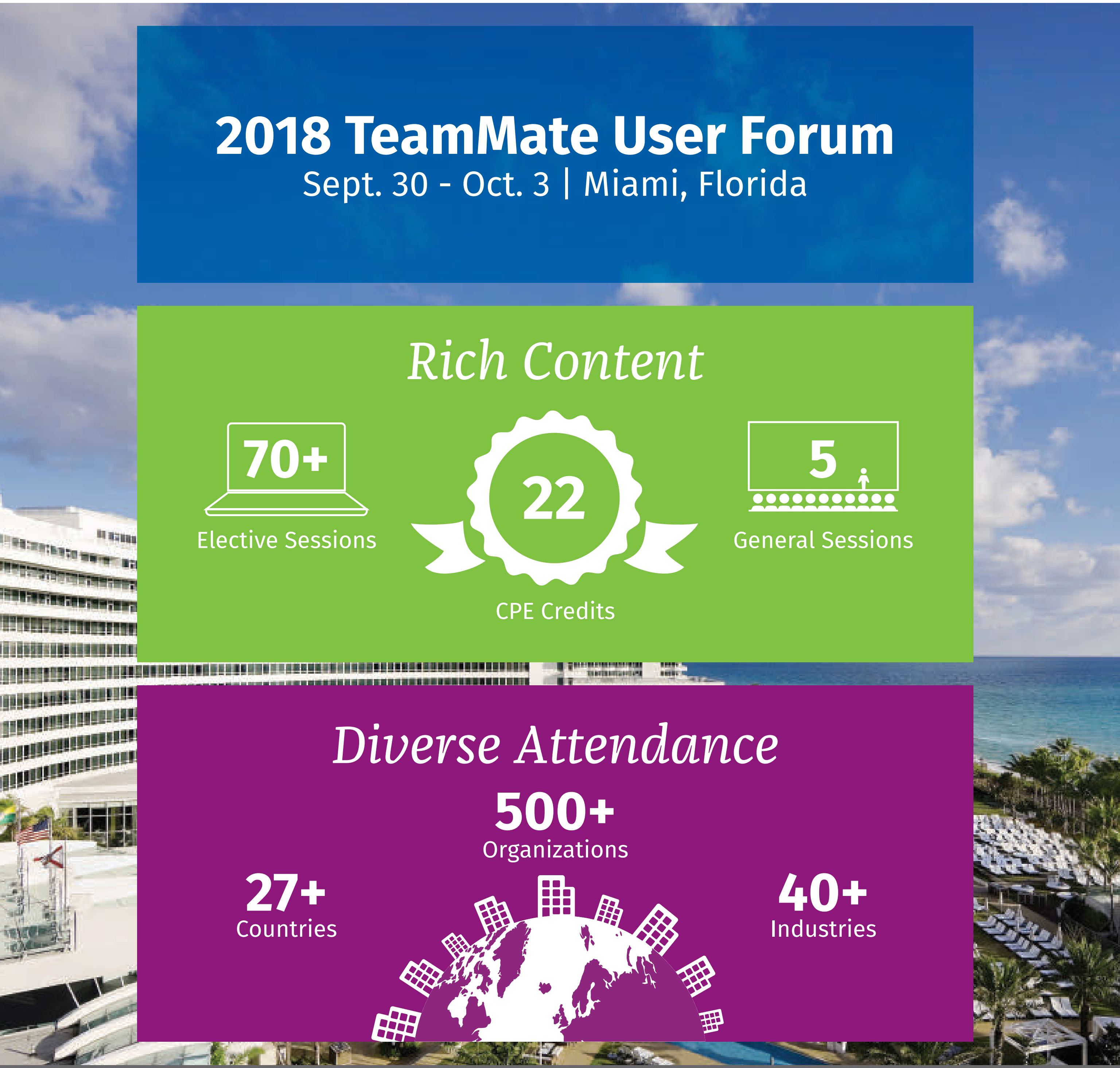
BUILDING INTELLIGENCE

Bible and McLaughlin both advise internal audit departments to start with a small project, before expanding their use of AI tools. That goes for the organization, as well. Organizations first will need to take stock of their data assets and get them organized, a task where internal auditors can provide assistance.

For audit executives such as Gurman, the objective is to get up to speed as fast as possible on AI and all its related risks, so they can educate the audit committee and the board. "There is a lot of unknown," she concedes. "What risks are we bringing into the organization by being more efficient and using robots instead of human beings? Use of new technologies brings new risks." Ia

TIM MCCOLLUM *is* Internal Auditor*'s associate managing editor.*

Wolters Kluwer



2018 TeamMate User Forum

Sept. 30 - Oct. 3 | Miami, Florida

Rich Content

70+ Elective Sessions

22 CPE Credits

5 General Sessions

Diverse Attendance

500+ Organizations

27+ Countries

40+ Industries

Get practical knowledge that will have an immediate impact on your day-to-day activities while earning CPE. **Register by Dec. 31 and save $400.**

Learn more: TeamMateUserForum.com

Risky Relationships

A holistic audit strategy can provide confidence in the performance of third-party partners.

Ben Arnold
Alistair Purt

Third parties are becoming increasingly important to succeeding in today's complex business environment. Many organizations are assessing their core strengths and turning to a diverse range of outside organizations where specialist capabilities are required. While such relationships can give organizations a competitive advantage, they also can impact their reputations.

Like all business relationships, trust is integral in working with third parties. Internal auditors can help their organization ensure that trust is fostered and maintained. Moreover, they can assess whether the organization has established effective processes to support its third-party relationships.

A HISTORY OF SETBACKS

Using third parties has its risks. Choosing a partner and determining the type of contractual arrangement to put in place can be difficult because of the range of options available (see "Third-party Relationships and Impacts" on page 33).

Once chosen, there is no guarantee that the third-party relationship will succeed. There are numerous examples where the actions of third parties have significantly damaged the reputation and financial strength of the contracting organization. In these instances, competitors press their advantage.

TSKJ A joint venture formed by the U.S.'s M.W. Kellogg Co. (now known as KBR), France's Technip, Japan's JGC, and Italy's Snamprogetti, TSKJ won four contracts worth

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

more than $6 billion between 1995 and 2004 to design and build liquefied natural gas facilities on Bonny Island, Nigeria. None of the participants had a majority stake in the joint venture. TSKJ reportedly used agents to bribe Nigerian government officials, and the U.S. Securities and Exchange Commission (SEC) initiated the case in 2009. The SEC declared that each joint venture partner had culpable knowledge of the payments because senior executives from each company, including some who were serving on the TSKJ steering committee, participated in meetings where the bribery was discussed.

The four companies paid a combined $1.7 billion in civil and criminal sanctions for the decade-long bribery scheme. These include: Snamprogetti and its parent company ENI paid $365 million; Technip paid $338 million; and consortium leader KBR and its former parent Halliburton paid $579 million.

The supermarkets lacked visibility across the supply chain.

The nonfinancial impacts in this case included reputational damage and criminal charges against current and past joint venture parent employees. KBR's U.S. Foreign Corrupt Practices Act (FCPA) violations impacted successor liability after Halliburton acquired KBR in 1998. These were based on book and record violations and Halliburton's lack of post-acquisition vigilance. On the financial side, the FCPA and U.K. Bribery Act investigations affected share price and capitalization for all the companies.

Supermarket Cyberattack In 2013, a cyberattack of a U.S. supermarket chain impacted an estimated 40 million customer debit and credit cards. A phishing attack was used to gain access to the company's network and compromise a third-party vendor. The chain suffered significant reputational damage. The cost of the breach was an estimated $202 million, and the chain paid $18.5 million to settle legal claims by 47 states.

Food Contamination In January 2013, news outlets reported that foods advertised as containing beef contained undeclared or improperly declared horse meat—as much as 100 percent of the content in some cases. This initially was discovered by the Food Safety Authority of Ireland, who found horse DNA in frozen beef burgers sold in several Irish and British supermarkets. Investigations uncovered complex supply chains—one involved eight separate vendors and traders across five European countries. The supermarkets lacked visibility across the supply chain and did not have suitable controls to verify the end product.

The supermarkets' reputations suffered significantly, with financial repercussions as well. A U.K. House of Commons report stated, "The evidence suggests a complex network of companies trading in and mislabeling beef or beef products, which is fraudulent and illegal."

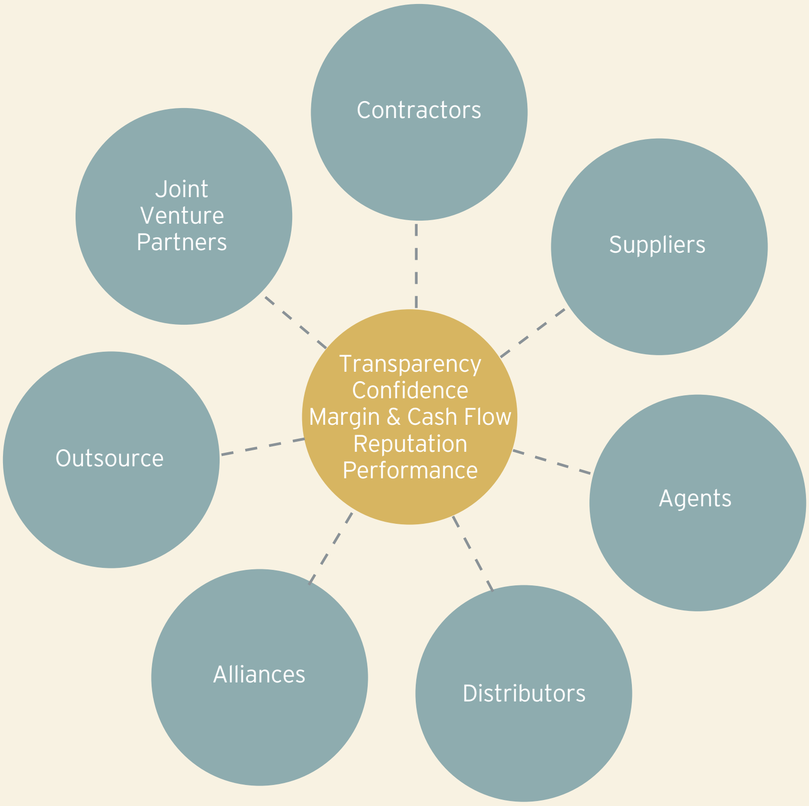
THE IMPORTANCE OF AUDIT PLANNING

Third-party trust features in most audit plans, whether it's part of a review, a review of the third party, itself, or a holistic third-party governance framework audit. Understanding the organization's risk profile/supply chain and benchmarking against a third-party governance framework can help internal audit address the correct risks, prevent adverse outcomes, and add value to management. Whether auditing individual activities or an entire third-party governance framework, auditors can compare them with the elements of the "Third-party

> Only 50% of audit professionals described their organization's monitoring of the activities of existing third-party service providers as adequate or strong. —2017 IIA Pulse of Internal Audit Survey

THIRD-PARTY RELATIONSHIPS AND IMPACTS

Third parties have a direct impact on the organization's objectives. Successful relationships can lead to large upside; however, there also are many risks that need to be understood and mitigated.



Governance Framework" on page 35 to identify improvement areas.

PLAN

With a vast range of partnership structures and operations across industries, implementation of a governance process can be challenging. Risk management within trust relationships will depend on the nature of the relationship, including level of influence, ownership/management control, and the third parties' appetite for control monitoring and risk management. Questions to ask include:

- Is the organization able to perform the service in-house?
- Has the organization performed appropriate due diligence before third-party engagement?
- Has the organization prioritized and ranked its third-party relationships according to risk?
- Has the organization selected the correct type of third-party relationship, such as an alliance, joint venture, or contract?
- Will the third-party represent the organization effectively and align with its culture?
- Does the third-party contract include an audit clause?

Audit objectives include:

- A clear vision and third-party strategy for service delivery.
- Consistent third-party governance structure design.
- A risk stratification model.
- Due diligence procedures, including cultural alignment.
- Design and use of a risk-based, standard contract template.

EXECUTE

Internal audit typically perceives the execution phase as having the most direct impact on performance. Auditors should assess whether there are processes to support working with third parties to achieve shared objectives. Audit questions include:

- Is there clear stakeholder and role definition for all aspects of the contract life cycle?
- Do all of the relevant personnel have the appropriate knowledge, skills, and experience?
- Are established performance metrics based on identified risks?
- Is cultural alignment continually reinforced?
- Are technology and data being used as effective enablers to manage the relationship?
- Does the provision of information between partners align with anti-trust requirements?

Audit objectives include:

- Timely identification and resolution of issues.
- Effective performance management throughout the contract life cycle.
- Timely, accurate, and transparent third-party reporting.
- A joint culture of continual improvement within the organization and the third party.

MONITOR

Third-party assurance often focuses on how the third party is directly managed. It also is important to

NAVEX GLOBAL®
The Ethics and Compliance Experts

Protect your organization against legal, reputational and financial risk with RiskRate:

- Automated Screening Process
- Continuous Due Diligence Monitoring
- Flexibility Where You Need It
- Optional Analyst-Driven Reports

Learn more about RiskRate today **www.navexglobal.com/RiskRate**

RISKRATE™
Enterprise Due Diligence

www.navexglobal.com | +1 866 297 0224 | info@navexglobal.com

© 2017 NAVEX Global, Inc. All Rights Reserved.

MORE VISIT our mobile app + InternalAuditor.org to watch a video on third-party risk.

THIRD-PARTY GOVERNANCE FRAMEWORK

This third-party governance framework demonstrates a benchmark used by organizations that are effective in managing third-party relationships to successful and mutually beneficial outcomes.

1. Plan
Determine which third parties you need and how these should be structured to derive maximum benefit to your organization.

3. Monitor
The reporting and assurance mechanisms used to monitor the success of third-party arrangements.

2. Execute
End-to-end management of third parties to ensure you are collaboratively working toward the achievement of shared objectives.

4. Improve
Identification and action of issues identified, both for individual third parties and for your overarching management framework.

understand how it is monitored and assessed. In large, complex organizations, this involves understanding how responsibilities are split between the first and second lines in the three lines of defense.

The audit also must consider how management uses data to ensure effective monitoring. Organizations often generate significant volumes of complex data but do not always use it effectively. Auditors should ask:

- Have key risks been factored into third-party assurance?
- What level of assurance is required and can third-party assurance reports be used?
- What assurance is provided by the second line of defense?
- Have data-based key performance indicators (KPIs) and red flags been identified? Are they continually monitored, with management taking action where poor performance is identified?
- Does the third party have effective assurance mechanisms?

Audit objectives include:

- Risk-based assurance model.
- Scope covering end-to-end third-party risks, such as subcontractors.
- Analytically driven contract compliance program.
- KPI-based dashboard reporting, including red flags.

During this stage, internal audit should look for warning signs such as whether management is identifying and taking action on red flags. Examples include:

- Safety: safety incidents, a high number of recordable injuries, and significant audit findings.
- Performance: missed KPIs, disrupted service, and poor third-party governance.
- People: high turnover, poor culture and tone at the top, and reduced capacity and capability.
- Information: data leaks, bad press, and regulatory breaches.

IMPROVE

To achieve effective third-party relationships, areas for improvement must be identified, communicated, and resolved so problems do not escalate. Management and assurance activities often overlook this phase. Improvement should be continual and can be applied to individual third parties and the overarching governance framework. Internal audit should assess whether this is being undertaken by asking:

- Are contract managers sufficiently trained to embed continual improvement?
- Are issues used to drive improvement actions?

Internal auditors are not just a bunch of rule followers.
We're solution-focused and principle-minded. Standards-driven, framework-followers. As a matter of fact, global industry experts at The IIA develop, document, and deliver the standards of the profession. The *International Standards for the Professional Practice of Internal Auditing* help all internal auditors be more effective.

You won't believe how helpful it is to have standards.

Standards Practice Makes Sense
www.theiia.org/WeHaveStandards

The Institute of Internal Auditors

2017-0470

IT services, business services, and equipment vendors are the most significant third parties in organizations' business models. —2017 IIA Pulse of Internal Audit Survey

- Is the effectiveness of the framework monitored through the use of portfolio-based metrics?
- How often are overarching processes controls reviewed?
- Are third-party outcomes routinely successful?

Audit objectives include:

- Improvement actions are routinely implemented.
- A joint culture of continual improvement is in place.
- The third-party governance framework is systematically evaluated and improved.

ACHIEVING SUCCESS

Collaboration, communication, and engagement are key to sustaining third-party relationships. Key principles for sustainable success are:

- Establish strong leadership and sponsorship.
- Involve third parties early.
- Develop agreements that include two-sided incentive plans.
- Identify continuous improvement opportunities.
- Align benefit realization to strategic objectives.
- Collaborate on product and service design.
- Engage in joint process improvement.
- Integrate systems and apply technology effectively.
- Establish shared KPIs focused on outcomes.

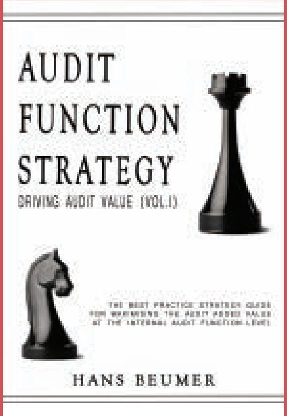
Third parties can cause significant exposure and adverse consequences to an organization's objectives. Implementing and assessing a governance framework will maximize the opportunity to mutually achieve strategic objectives.

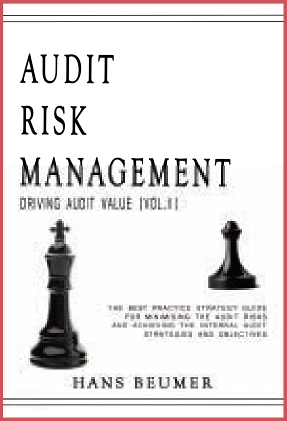
Risk management and internal audit should be active in third-party governance, from thought leadership and support during strategy development to controls monitoring, execution of third-party audits, and follow-up. The right audit and risk process will include thought and definition around risk exposures and the implementation of risk performance criteria and monitoring. Continuous monitoring throughout the process will help ensure appropriate oversight of, and ultimately comfort with, third parties.

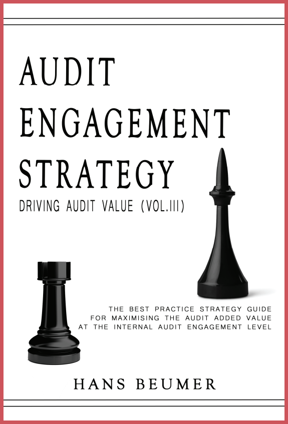
BEN ARNOLD, CIA, CA, CFE, FGIA, *is based in Perth, Australia.*

ALISTAIR PURT, ACA, FCA, *is a director at A&P Advisory in Perth, Australia.*

NEW - IA BEST PRACTICE STRATEGY GUIDES


AUDIT FUNCTION STRATEGY
DRIVING AUDIT VALUE (VOL.I)
THE BEST PRACTICE STRATEGY GUIDE FOR MAXIMISING THE AUDIT ADDED VALUE AT THE INTERNAL AUDIT FUNCTION LEVEL
HANS BEUMER


AUDIT RISK MANAGEMENT
DRIVING AUDIT VALUE (VOL.II)
THE BEST PRACTICE STRATEGY GUIDE FOR MINIMISING THE AUDIT RISKS AND ACHIEVING THE INTERNAL AUDIT STRATEGIES AND OBJECTIVES
HANS BEUMER


AUDIT ENGAGEMENT STRATEGY
DRIVING AUDIT VALUE (VOL.III)
THE BEST PRACTICE STRATEGY GUIDE FOR MAXIMISING THE AUDIT ADDED VALUE AT THE INTERNAL AUDIT ENGAGEMENT LEVEL
HANS BEUMER

Maximising internal audit added value at the internal audit function level
ISBN 9783906861135

Minimising internal audit risks to achieving internal audit strategies and objectives
ISBN 9783906861159

Maximising internal audit added value at the internal audit engagement level
ISBN 9783906861180

Available in Print and EBook, at the IIA Bookstore, www.theiia.org/Bookstore or Amazon, Lulu, iBook Store, Barnes Noble, Ingram

Beyond the

ILLUSTRATION BY SEAN YATES

“Internal auditing should be about tomorrow,” Charlotta Hjelm, chief internal auditor at the Swedish insurance co-operative Länsförsäkringar, Stockholm, says. “If the function focuses mainly on financial audits, it is mostly looking at what happened yesterday and today.”

Hjelm says boards and audit clients are looking to their chief audit executives (CAEs) to provide assurance over their forward-looking operations and strategies—no more so than in areas of rapid change, such as product launches or IT initiatives. As a result, functions that have historically concentrated on auditing controls over financial information have been pushed out of their comfort zones and into the fuzzier world of nonfinancial auditing.

“If you are conducting financial audits, things are black and white,” Hjelm says. “The controls are right or wrong.” So-called nonfinancial audits, on the other hand, may be concerned with improving the efficiency of business processes, or the quality of services. Auditors working in those areas need adequate knowledge

numbers

Auditors can help ensure nonfinancial information is delivered to the stakeholders who need it.

Arthur Piper

of the business and its functions—from human resources and sales, to supply chains and customers. "If a business wants to be the best, most efficient, and offer the highest quality of goods or services, that can be hard to define," she says.

This lack of clarity has an impact on internal audit. If an organization's goal setting is not precise, auditors can struggle to grasp what separates the most important audit area, for example, from the slightly less important. Moreover, risks in dynamic areas of the business can change rapidly, impact business processes in other parts of the business and prove difficult to cover comprehensively. Internal audit teams working in nonfinancial areas of the business need a wider range of technical skills, broader soft skills, and deeper business knowledge. But the rewards of engaging in these areas include providing better insight to the business on the quality of its operations and the risks it faces tomorrow.

ALIGNING WITH THE BUSINESS

The shift in emphasis from static, backward-looking audits has come from boards and from the profession itself as it has sought to win that coveted seat at the top table. In fact, over the past 15 years internal auditors in most sectors have been aligning themselves more closely with their organizations' strategies. According to Driving Success in a Changing World: 10 Imperatives for Internal Audit, a 2015 report from The IIA containing the most recent figures, globally 57 percent of audit departments say they are aligned fully or mostly to their business' goals and objectives. As that percentage continues to grow, increasing numbers of auditors will be moving into those dynamic areas of the business that need assurance most—whether they are primarily financial in nature or not.

This realignment to auditing nonfinancial areas has led to a shift in approach that places greater value on what audit findings mean to the business than whether or not the organization is compliant with regulations. In regulated areas such as finance, for example, boards still want to know whether they are compliant with Solvency II—a European Union directive that focuses primarily on capital obligations for insurance firms—where there is a clear role for traditional internal audit, Hjelm says. "But they also want to know how much it will cost, whether we have the resources to do what is necessary, how it will affect the strategic plan, and whether I have audited the right areas." Communicating on

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

> “When you say ‘business acumen,’ do you mean that people understand the way things are done, or the way they should be done?”
>
> Phil Tarling

such a wide range of issues clearly has become an important dimension of Hjelm’s work.

Malcolm Zack, who has led audit teams in the consumer, payments, foodservice, mail, entertainment and travel sectors and now heads Zack Associates, an internal audit consultancy based in London, says he has been auditing nonfinancial areas of the businesses in which he has worked for more than 20 years. Over that time, he has worked across a range of areas including IT audit, contingency planning, health and safety, codes of conduct, supplier risk, buying and merchandising, and social media, to name just a few. But he agrees with Hjelm that more recently boards have been encouraging internal auditors to move into areas where the business is changing rapidly because that is where the big risks can be.

“In recent years, I’ve been working more and more on business change projects, and project and program assurance,” he says. “New products and systems are where the higher risks are, and the ongoing auditing of those has become very important.”

Trends in nonfinancial auditing areas are coming under the spotlight.

He sees that trend intensifying in the coming years with auditors becoming more focused on the commercial and operational significance of their findings in such dynamic areas, rather than just on the financial data itself. Because finance is only one element the board needs assurance on, Zack says, that has changed the composition of many audit teams away from accountants and pure audit specialists. Experts in project management, IT, or human resources, for example, could be needed as much as technical auditing ability. An audit team in one financial institution Zack was familiar with, for instance, employed psychologists on its team during an audit of its culture.

“This has been a shift for the profession,” he says. “We are being asked to give a view of risk and controls across the entire organization potentially.” That requires the audit team to be staffed by a core of experienced auditors supported by a more fluid mix of people from different specialist areas and cultures to provide depth of knowledge in the area being audited, he says.

SHIFT IN FOCUS

The difference between a financial audit and a nonfinancial audit can be one of focus, explains Phil Tarling, an internal audit consultant based in South East England, U.K., and former vice president, Internal Audit Capability, and head of the Internal Audit Centre of Excellence at global telecommunications firm Huawei Technologies. In one supply chain audit he was involved in, for example, when goods did not ship in time by sea, they were sent at greater cost by air. The financial findings were significant, but the nonfinancial part of the audit also showed that the supply chain was poorly structured and included recommendations on how to fix the problem.

“In nonfinancial auditing, you need people to understand that the business exists to make a profit and that cost has a negative impact on its ability to do so,” he says. “Not all auditors think that way, and not all people working in the business do either.”

That is why Tarling is cautious about bringing people with business acumen, or with subject-area expertise, into the audit function. “When you

> “You can be the facilitator that helps join the dots across the whole organization and beyond.”
>
> Karem Obeid

Four out of five global investors say companies do not adequately disclose nonfinancial risks that could affect their business, according to a 2017 EY survey.

say 'business acumen,' do you mean that people understand the way things are done, or the way they should be done?" he asks. He warns that external staff from the business can bring with them negative baggage and may be too caught up in the minutiae of their role to see the bigger picture, or to imagine different ways of working.

"It means you have to work a lot harder to get the right people on the audit team," he says. Going back to his supply chain example, he would recommend hiring someone who possesses high-level experience with establishing a supply chain and training him or her in audit and risk. Smaller audit functions would need to cosource such staff with an internal audit provider and transfer knowledge to the core team during the project, he says.

Integrated thinking needs to serve a wider range of stakeholders.

INTEGRATED THINKING

Trends in auditing nonfinancial areas are coming under the spotlight from regulators, standard setters, and business groups mulling over the causes of the financial and economic crash of 2007—the effects of which are still felt today in the form of historically low interest rates and slow growth in many countries. The consensus among groups such as the International Integrated Reporting Council (IIRC) is that many businesses did not understand how the risks within their businesses are related to each other and to the wider business world. Providing some form of coordinated assurance over all nonfinancial aspects of corporate activity can be achieved by integrated reporting (<IR>).

The IIRC's International <IR> Framework argues that, too often, companies have disjointed reporting practices that are driven more by regulation than by business need. That has led to a fragmented approach to what is reported. What is needed, the framework says, is <IR> delivered to shareholders and stakeholders that provides a complete picture of the business and its risks, which is underpinned by integrated thinking.

"Integrated thinking is the active consideration by an organization of the relationships between its various operating and functional units and the capitals that the organization uses or affects," the framework says. "Integrated thinking leads to integrated decision-making and actions that consider the creation of value over the short, medium, and long term."

The IIA recently articulated internal audit's potential role in the integrated thinking arena. Its project concluded that internal audit's holistic purview of the organization uniquely positions it to support integrated thinking's goals of strategic decision-making, planning, and delivery in a way that considers the perspectives of the business, its various stakeholders, and the resources needed to create wealth.

"Internal auditing is focused on the same central concerns that prompt the move toward integrated thinking and enhanced external reporting," says Anton van Wyk, a former IIA board chairman who led the organization's integrated reporting task force. "By providing well-informed insight, advice, and assurance, consistent with The IIA's Core Principles for the Professional Practice of Internal Auditing, internal auditors can have a significant contribution to make in supporting their clients in their journey to integrated thinking."

CONNECTING THE DOTS

Some practitioners agree. Karem Obeid, CAE, Tawazun Economic Council in Abu Dhabi, United Arab Emirates, says boards have become more sophisticated in their understanding of what internal audit can offer—especially the function's ability to create value by driving business improvement and advising on risk in dynamic areas of the organization. "If as an auditor you get involved in benchmarking integrated thinking and reporting at an early stage," Obeid says, "you can be the facilitator that helps join the dots across the whole organization and beyond."

He sees taking on the role of driving the integrated thinking project as a great way of demonstrating the value that internal audit can add to the business. It can also help the audit team better direct its work and resources to where they are most needed, and enable internal audit to serve the organization as a trusted advisor.

Auditors can do this by building on their experience of auditing nonfinancial areas of the business, says Obeid—who contributed to the IIA white paper, Global Perspectives and Insights: Beyond the Numbers—Internal Audit's Role in Nonfinancial Reporting. But, he adds, integrated thinking is a project that has challenges. The CAE and his or her team, for example, must understand the business both from a technical and practical point of view. Those with many years of nonfinancial audit experience will be better placed to see how the risks in different areas—often called silos—are related and how they may be audited across the business. Others would require a steep learning curve.

Second, integrated thinking and the reporting it produces need to serve a wider range of stakeholders—both within and outside the business. Although most internal auditors are effective at dealing with the board, management, and some other functions—such as risk and compliance—few have experience in dealing directly with external stakeholders, such as customers and external pressure groups.

"Internal auditors need to communicate more with stakeholders, not just through business meetings, but through social media, socializing in person, and getting to know the culture and mindsets of these groups," Obeid says. "Also, the audit team has to increase among those groups an awareness and understanding of audit's role—and the importance of following The IIA's *Standards*."

SUSTAINABILITY

One area of rapid change in the integrated reporting world is that of climate-related financial disclosures. Although a paper published in June by the U.S. Financial Stability Board (FSB) relates to financial services businesses, it is a good example of how important governments now view the environmental impact of investor decisions on society. The paper, Task Force on Climate-related Financial Disclosures: Overview of Recommendations, proposes enhanced, voluntary disclosures on how each organization's governance, strategy, risk management, and metrics help it report accurately and effectively on climate-related risks.

For Richard Goode, an executive director in the Americas Climate Change and Sustainability Services practice at EY, the paper is a clear indication of how government agencies and investors are increasingly asking to see proof of an organization's "social license to operate." According to the EY Center for Board Matters, more than half of the shareholder proposals during the 2017 proxy season related to environmental and social issues—in other words, pressure is growing for companies to demonstrate their social, ethical, and environmental credentials.

"This is a key area for internal audit to act as a trusted business advisor," he says. "Business managers are asking internal auditors to help them articulate what their nonfinancial risks are and how well their sustainability programs are being put in place and run."

Goode adds that while internal auditors can take a leading role, they should avoid an emotional plea to senior leadership and the board. "Speak the language of risk, collate and analyze the data, benchmark within your industry and among standout performers in other industries, and prove what is important and why."

TRUSTED NONFINANCIAL ADVISOR

Goode stresses the importance of having the right expertise to help tackle the more technical aspects of such nonfinancial areas. On the other hand, the lack of such expertise should not be used as an excuse for inaction.

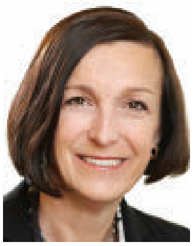
"Make sure you get the topic on the risk register and talk to the business about what risks they are facing in that area," he says. "Talk to managers, institutional investors, and stakeholders and put together an honest materiality assessment." If the risk is real and material, the resources are likely to follow, he adds.

Hjelm agrees. "The more success you have in these nonfinancial areas, the more trusted you will be to do less testing," she says. "You will be providing true insight for the company about their potential future risks and helping the company make money tomorrow. Besides, as an internal auditor it's much more rewarding to help people and have fun while doing it." Ia

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

"Business managers are asking internal auditors to help them articulate what their nonfinancial risks are."

Richard Goode



"The more success you have in these nonfinancial areas, the more trusted you will be to do less testing."

Charlotta Hjelm

Agile Performer

FRANKIE'S / SHUTTERSTOCK.COM

Prompted by rapid organizational change, the CAE at a multinational insurance firm adopted a radically different audit model.

Ruth Prickett

Ralph Daals, group chief auditor of London-based RSA Insurance, is passionate about the journey he and his team have been on over the past two years. "The seeds for the transformation were sown in October 2013 when internal audit uncovered significant irregularities during a routine review in our Irish business," he explains. "That event was publicly reported and brought home the message that, in the end, internal audit will be judged by the things it misses."

This clarity about internal audit's accountability led to new, forward-looking expectations of the function. Daals recalls: "Our chairman put it nicely—'I would like you to be able to tell me that the building is about to catch fire, as opposed to pointing me to it after the event.'"

Meanwhile, RSA was transforming with an agenda of significant strategic rationalization, cost reduction, and operational turnaround. The company was changing rapidly with innovations around big data, robotics, and more digital and agile developments; and with these changes a new profile of risks emerged. "Typically, internal audit follows the company," Daals says, "but we were driven to make a huge leap to get ahead and stay ahead."

The challenges were tough. "We not only had to become more dynamic and forward-looking, and get on top of the new risks RSA was facing, but we also had to play our part from a cost and efficiency point of view. We had to do more with less—we're talking about a double-digit percentage cost reduction here," he says. "Doing this right meant reinventing ourselves and fundamentally changing our mindset, skills, and ways of working."

TRANSFORMING INTERNAL AUDIT

The ambitious changes Daals sought required the function to be inventive—particularly because, he emphasizes, it did not have deep pockets and could not hire expensive consultants. "Constraint was a key driver of innovation and, ultimately, became a real friend," he says.

The team started to assess the world around it, identifying and learning from cutting-edge companies regardless of industry and function. "We ended up casting the net pretty wide and then adopting and tailoring what we thought could work well for us," Daals says. "Jim Collins' book *Good to Great* provided a lot of early inspiration. It was all about starting with purpose and people—attracting and retaining the right talent, giving them freedom within a framework, and playing to their strengths."

He was wary that, in too many cases, change programs introduced new processes that existed on paper, but didn't lead to new ways of working in the long term. Theirs was not, he argues, a traditional transformation program—it had no project plans, no champions, and no reams of documentation.

The ambitious changes Daals sought required the function to be inventive.

"We looked to make change easy and infectious, with small iterative improvements driven by obsessing over the right things: sharing successes, challenging each other, and ultimately deeply embedding practices and improvements in our behavior and culture," he says. "At any time we have about five functionwide 'obsessions,' both behavioral and technical. These create a ripple-effect-based transformation—contagion can be very powerful."

This approach allowed people to see and feel the build-up of momentum and meant that evolution could happen at an increasing—and often surprisingly rapid—pace. Daals explains that he borrowed from computer animation firm Pixar's innovation culture and started to experiment, test, and refine ideas.

BUILDING BLOCKS

The transformation rested on four main interconnected "building blocks." The first of these was to simplify and standardize what the team did and when it did it. This was intended to minimize complexity and distractions to allow internal audit to focus all its time and efforts on what mattered most. A vital part of this process was that internal audit had to be comfortable about not doing some of the things it had taken on in the past. Daals says it started with "bonkers lists," which evolved into a functionwide learning exercise aimed at making the function more efficient and focused.

"We also wanted to keep it simple to ensure the real value comes from our core activities," he says. "We shouldn't have to resort to 'add-on' activities, such as advisory reviews, before value is created or recognized. It would imply something is fundamentally wrong."

The second building block involved increasing the relevance and timeliness of insights and interventions. The traditional annual planning process became a flexible six-plus-six rolling plan with a strategic three-year outlook. This allowed audits to run in parallel with changes in the business and emerging risks and to anticipate better the skills the team needed now if it was to be ready for the future.

At the same time, the team brought plan delivery in line with reporting to executives and nonexecutives, cutting the time between identifying findings and committee reporting to a minimum. "Our team now delivers 100 percent of our plan

Agile audit functions that are more closely **aligned** to the business at the point of disruption and risk help the organization better manage the risk event, according to PwC's 2017 Navigating Disruption study.

every quarter, which was unheard of in the past," Daals says.

The third building block involved implementing an "AsOne" operating model, inspired by Daals' past work with Deloitte. "We broke down the silos that typically exist in an international function and eliminated the traditional reporting structures and hierarchies," he explains.

RSA internal audit consists of more than 60 people based in key cities across three regions: the U.K., Ireland, and the Middle East; Canada; and Scandinavia. Daals says that the AsOne model "facilitates a high level of connectivity and collaboration between the teams" so they can work together as if they were all in the same room. This necessitated a new digital way of working and using communication channels such as Yammer.

"Building on AsOne, we advanced our way of working based on music streaming service Spotify's agile culture. We even adopted some of their naming conventions," Daals says. "We now structure ourselves around 'squads'—fluid teams that bring together the right people for an audit or other initiative, regardless of hierarchical position or location."

For the audit function's stakeholders, Daals says that AsOne increased the quality and consistency of output and coverage, improved the way internal audit shared best practice, and boosted efficiency by reducing duplication and, ultimately, cost.

The fourth building block was all about striving to build a high-performance culture. "This may sound clichéd—and many talk about it—but in the end we are a people business, and so building a high-performance culture was crucial," Daals explains. "For us, this is about striving to create an environment where we can attract and retain the best." He was inspired by Google's approach to investing in talent and its view that hiring remarkable people is its single most important activity.

"We tailored this—only people with the passion and aptitude for it are involved in recruitment," he says. "Our recruiters, typically our most senior people, dedicate significant time to finding the right talent. Every candidate is recruited with an international interview as standard."

Daals and his team also looked to elite sports for ideas. "We work closely with performance company PlanetK2, which uses the same kind of performance psychology ideas with us as it uses with Olympic teams. Everybody is challenged about how to get the best out of themselves and each other."

Agility needs to be embedded in the mindset, culture, and values of the team.

All these changes helped to create what Daals characterizes as an agile function. "Agility for us is about being dynamic and flexible. It is about our ability to anticipate, respond, and continuously improve." He adds that agility needs to be embedded in the mindset, culture, and values of the team; processes and methodologies then follow naturally. "It's about having a team that gets better and better with every challenge thrown at it," he says.

He says that this agility has many advantages: Internal audit is now better at using the team's full capabilities and experience, it can rapidly gather and deploy the right resources via the squads, and the rapid feedback between stakeholders and the function facilitates quick and constant improvements in what the function does and how it does it.

Accountability remained a focal point throughout the changes. "Our

MORE

To learn about RSA internal audit's recent awards for outstanding performance and innovation from the U.K.'s Chartered IIA, VISIT http://bit.ly/2ArW56l.

Leverage an External Quality Assessment in 2018

Build confidence with your stakeholders with a solid Quality Assurance and Improvement Program (QAIP). Look to IIA Quality Services' expert practitioners to provide:

- Insightful external quality assessment services.
- On-time solutions and successful practice suggestions based on extensive field experience.
- Enhanced credibility with a future-focused QAIP.

IIA Quality Services, LLC, provides you the tools, expertise, and services to support your QAIP. Learn more at **www.theiia.org/Quality**

IIA® The Institute of Internal Auditors

2017-1275

Nearly 50 percent of CAEs say process improvement and innovation are "very essential" or "extremely essential" internal audit skills, according to The IIA's 2017 North American Pulse of Internal Audit.

accountability is always front of mind," Daals says. "We regularly ask ourselves our killer question: 'Have we missed anything significant?'"

"To answer this," he continues, "we perform a half yearly exercise where we look back across our business through the lenses of issues raised by others, risk incidents, and material external events. We ask, 'Where were we?' 'Did we pick it up?' and if so, 'Did we report it appropriately?'" The lessons identified are widely discussed and fed into the continuous improvement of the function, and Daals says the results are getting better every time. He sees it as crucial to delivering against internal audit's purpose of keeping RSA safe and improving.

Daals also takes quality assurance seriously. He employs Deloitte to review and challenge audits done in the previous quarter. The reviewers assess whether the audits focused on the right areas and identified the correct risks and issues.

SKILLS FOR THE FUTURE

The new-style internal audit team needs to attract a new type of internal auditor, with skills that will be important to the organization of the future. This means it needs to offer an exciting proposition in terms of both working environment and opportunities, Daals says. New recruits may come from other sectors or have a nonaudit background. The team currently includes nontypical members such as a web and app developer and a criminologist. "It's important to get the balance right between maintaining their unique skills and perspectives and learning internal audit essentials," Daals adds.

His search for innovative people who are willing to be shaken out of their comfort zone and are eager to improve constantly is making the team more distinct and adept. "We are always asking how we can break through the typical talent barriers," he says. "We are well aware that what we are creating doesn't suit everybody, it requires tenacity and resilience. At times we have had to make some difficult decisions, but that's OK."

To help team members grow to their full potential, Daals has introduced innovations such as a dedicated "Learning Friday" every other month on which everybody can choose what they learn. No work is allowed.

"We took a lot of inspiration on how to create the best workplace from an [online education] company called Mindvalley," Daals explains. "It is important we not only bring in new skills, but make sure all our people are set up for the future. So we are investing in upskilling people in 'new world risks' such as cyber risks and risks arising from big data and use of robotics and artificial intelligence." This includes teaching them the basics of coding, how to audit agile developments, and simulating mock crises such as a cyberattack. Daals expects everyone to become highly proficient with data analytics tools.

The new-style internal audit team needs to attract a new type of auditor.

He also wanted to move away from a system where people couldn't progress until the person above them left. The new structure has no fixed number of people per level, so if someone is ready to be promoted, they can be.

HINDSIGHT AND INNOVATION

So what's next? "It has been good so far," Daals says. "Our feedback scores have consistently gone up and our people are in high demand by the business. We have a more agile and forward-looking model that we hope will help us to deal with whatever comes our way. But it doesn't stop here. We have identified, for example, seven ways of injecting innovation into auditing, including stress-testing the control environment and risk-event and scenario-based auditing. As long as it supports our purpose and we keep an appropriate eye on what we call 'audit risk,' we won't hesitate to give it a go."

He is keen, however, to stress that agile is not the same as chaos and needs careful management. He advises others looking at creating an agile culture to establish first a stable "backbone." You also need to find a way to combine opposites. "Looking forward is great, but not if you don't look backward at the same time," he warns. "Sustainability of controls and remediation activity is as, if not more, important." Chasing emerging risks or organizational change can be catastrophic if you don't focus on the areas that everybody takes for granted, but can still hurt the company.

Daals concludes: "We may get it wrong sometimes; you can't win without ever failing. But in the end, it's fun putting yourself out there. If you fail, fail and learn fast, but never compromise on outcome."

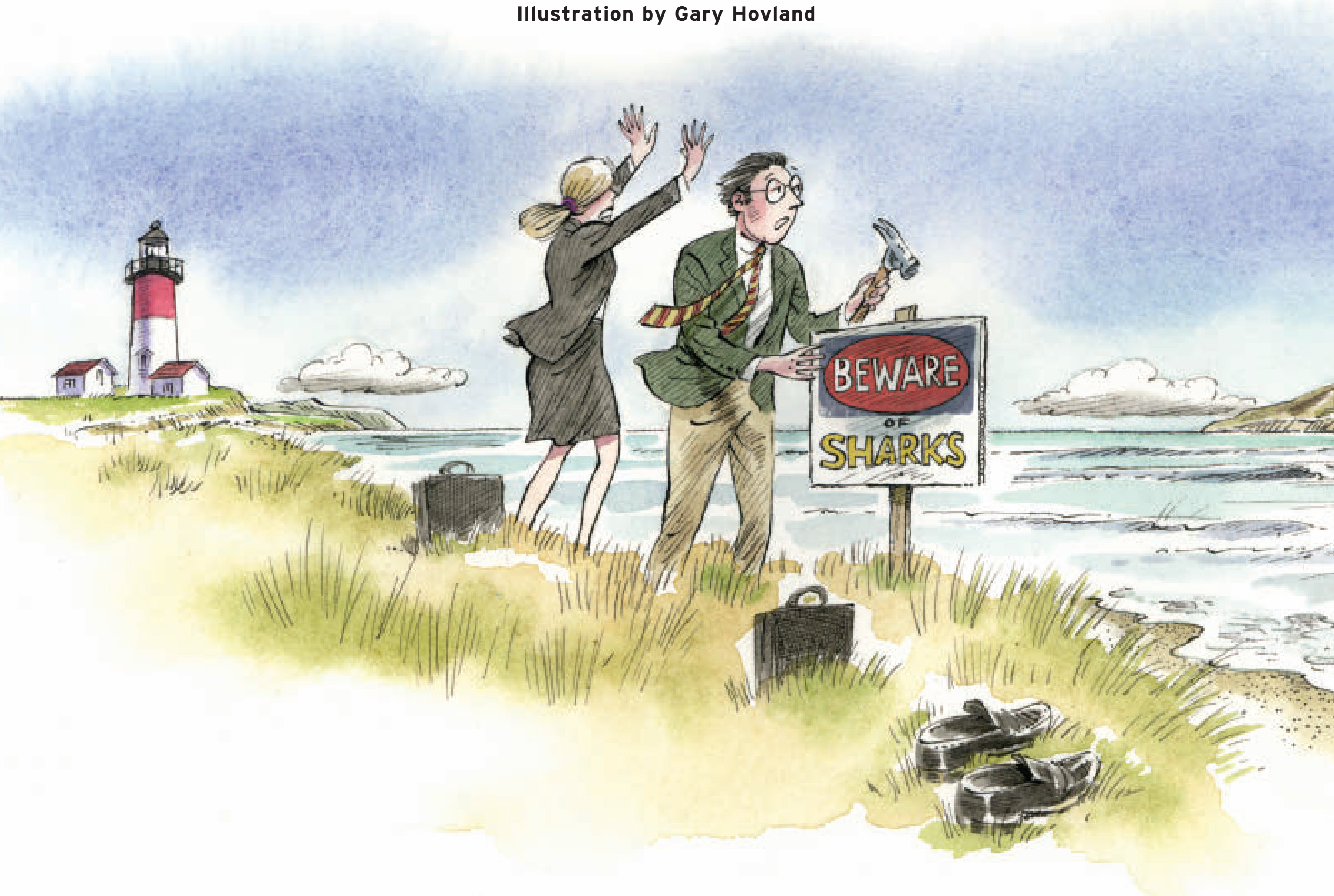
RUTH PRICKETT *is editor of* Audit & Risk *magazine.*

A version of this article first appeared in issue 36 of Audit & Risk, *the magazine of the Chartered Institute of Internal Auditors. Reproduced with permission.*

When recommendations go unaddressed

Jane Seago

Illustration by Gary Hovland



Internal audit needs to understand why recommendations aren't implemented to work toward a resolution.

The situation: An internal auditor makes a series of recommendations to an internal audit client, who refuses to implement one of the recommendations or address the finding.

The internal auditor's view: The recommendation covers an important point. Her supervisor agrees that the risk of not implementing the corrective action or addressing it would be significant for the organization.

The client's perspective: He concurs with the finding, but believes the corrective action would take too much time and use too many resources.

The outcome: After several unsuccessful attempts to persuade the client of the validity of the recommendation, the issue is elevated to the CEO. Lacking resolution with that step, the recommendation is sent to the audit committee. The internal auditor and her chief audit executive (CAE) attend the audit committee meeting to discuss the recommendation, gaining support from the committee and the chief financial

officer. The issue is resolved (ideally, the client attends the audit committee meeting and hears the committee's decision directly, but if that is not possible, the audit committee minutes can be used to inform the client) and a cordial working relationship continues.

Although the details of this scenario may vary, it likely describes a situation that is all too familiar to most internal auditors. The recommendations the internal auditor presents may not always be welcomed or feasible, but making those recommendations is integral to internal audit's role. That role, as Michael Levy, director of internal audit at Student Transportation Inc. in Wall, N.J., describes it, is "to spotlight issues and ensure that the appropriate people are aware and informed."

But raising awareness and sharing information do not always produce the needed results. An audit client may decline to implement even the most well-researched and clearly explained recommendation, leaving risks that may affect the organization's ability to achieve objectives unmitigated. When this happens, Standard 2600: Communicating the Acceptance of the Risk directs the CAE to discuss the matter with senior management or elevate the issue to the board, if necessary.

WHAT'S BEHIND THE "NO"?

As with many instances, when two parties fail to see eye to eye, inadequate or flawed communication may be to blame. In the case of unaddressed recommendations, perhaps the internal auditors did not fully explain the value of a recommendation, or they did not adequately define what "recommendation" means within the organization's culture, or they did not describe the potential consequences of failure to implement the recommendation.

Or, perhaps it is not a case of inadequate communication, but too much of it. "Many times, auditors tend to include every detail of the audit in the report," Levy says. "I find that executive management and the board are no longer looking for the 'novel' version of reports that has become common over the years." Internal auditors must focus on creating well-organized reports that stick to the point, covering what the reader needs to know, not everything the auditor knows. Each recommendation should be supported by a full description of the related risk, which will help establish the importance of the recommendation and the potential implications if it is left unaddressed.

"Executive management and the board are no longer looking for the 'novel' version of reports.

Michael Levy

Kevin Alvero, senior vice president of internal audit at Nielsen in Tampa, Fla., recommends using a categorization approach to clarify communication with the client. "If you clearly categorize recommendations based on risk (high, medium, low), you greatly reduce the chances that the most important ones will go unaddressed," he explains. "I think that is very intuitive to people: They understand that if they don't address the high-priority recommendations, there is a risk of that issue going forward." In an annual audit process, recommendations that appear multiple times may move to a higher risk category—a signal to management about their importance relevant to risk.

At Principal Financial Group in Des Moines, Iowa, Cindy Bolton, audit director, reports that implementation of an enterprise risk management framework has encouraged communication around risk and risk metrics by the chief risk officer (CRO) and all the risk officers throughout the business. "We have a lot of discussion about risk and controls from the second and third lines of defense, as well," she adds, "and a lot of time working in partnership with the second line, so the message to the first line is one continuous stream."

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

Besides communication, another possible reason for nonimplementation relates to resources. The benefits to be derived from the recommendation may not justify its cost, in the eyes of the client. Or the drain on other, nonfinancial resources may be prohibitive (although, if the recommendations are focused on issues that exceed the organization's established risk tolerance, this should justify adding resources). Auditors have a responsibility to understand the business well enough to be aware of the financial impact of the recommendations they are making. "Otherwise," Alvero says, "they are not fully serving the needs of the client."

When building an understanding of an issue that will be included in the audit report, internal auditors need to consider the cost, impact, and significance related to the issue. This enables the auditor to balance the high cost to remedy and the possible low impact and likelihood of misstatement the issue may potentially have. Although the internal auditor should definitely take the lead in these considerations, it should not be a solitary exercise. The client should play an active role.

Avoiding the cost-benefit objection can be as simple as discussing with the client the feasibility of various approaches and devising a management action plan in conjunction with management. When those discussions are held, the result "is not 'internal audit recommends and management responds,'" Bolton says. "Management is already involved."

If the cost of a recommendation is unknown, an approach might be to divide it into two parts: management researching the cost of possible solutions and internal audit determining whether these solutions adequately address the recommendation. This enables progress to be made, rather than hitting a brick wall of "no" the minute the cost is considered. Another workaround for expensive recommendations is for internal audit to make additional recommendations (such as extra reviews and quality reviews) to satisfy them.

"If they don't address the high-priority recommendations, there is a risk of that issue going forward."

Kevin Alvero

Communication and resources are not the only roadblocks to implementation.

"Developing recommendations is one of the areas where we, as a profession, have an opportunity to act as consultants and not only add value directly to the organization, but also to our stakeholders," Levy notes. "Many times, when recommendations are developed in a vacuum, without management's input, the desired outcome is not reached."

Communication and resources are not the only roadblocks to implementing recommendations. Kevin Patton, director of internal audit at The Ohio State University in Columbus, points out that a client's adoption of a recommendation may be affected by changes to existing information systems or implementation of new information systems, which often take longer than estimated. "System issues seem to take more time to resolve than other comments, such as financial and operational," Patton explains. "In those cases, we ask the unit how they are mitigating the risk and get an understanding of their processes." In some companies, moving to a new platform could make a recommendation obsolete, causing management to decide a short-term fix is not worth the cost. As with costly recommendations, the auditor should understand

the business well enough to be aware of systems plans before making a related recommendation.

Other possible situations that may affect the client's willingness or ability to implement a recommendation include a change in business strategy, loss of staff or changes in staffing, or competing priorities in the client's area. Ongoing communication with clients is critical to internal audit's effectiveness in such circumstances. It will help ensure that the internal auditor is informed on the client's issues and can function as a partner in addressing them.

THE FINE ART OF FOLLOW-UP

IIA Standard 2500: Monitoring Progress states that the CAE "must establish and maintain a system to monitor the disposition of results communicated to management." Item 2500.A1 speaks of the CAE's responsibility to establish a follow-up process to monitor and ensure that management actions have been implemented or senior management has accepted the risk of not doing so. Item 2500.C1 specifies that it is internal audit's responsibility to monitor (to the extent agreed with the client) the disposition of results of consulting engagements.

Failure to implement recommendations exposes the organization to risk.

Whatever the reason for failure to implement internal audit recommendations, that failure has the potential to expose the organization to risk. Therefore, internal audit has a distinct role in monitoring whether management implements the controls it agreed to. While the size and nature of the risk will influence the type and amount of follow-up activity, Following Up Recommendations/Management Actions, a 2016 paper from the U.K.'s Chartered Institute of Internal Auditors, outlines general post-recommendation activities that need to be made clear to the client before the audit:

- How outstanding recommendations/management actions will be tracked.
- How resolutions will be reported and validated.
- What follow-up action might be needed.
- How this will be carried out to provide assurance that identified risks are being addressed appropriately.

"If we have an audit with significant findings ... we automatically schedule a follow-up audit."

Warren Hersh

Warren Hersh, auditor general at New Jersey Transit in Newark, says a robust follow-up process must begin with the establishment of the department's verification philosophy, which generally will follow one of two approaches: 1) actually performing a follow-up audit, testing to verify that corrective actions have been implemented; or 2) accepting the representation of management on the status of corrective actions. In Hersh's experience, following the first approach takes significant resources and focus. His current department uses the second approach, with one variation. "If we have an audit that has significant findings that impact the key risks faced by the department, in addition to reporting to the audit committee, we automatically schedule a follow-up audit either later in the audit plan year or in the next audit plan year."

Hersh's team uses audit management software to monitor the status of corrective actions, and that status is reported at every audit committee meeting because it gets the attention of senior management.

MORE To read the Practice Guide, Audit Reports: Communicating Assurance Engagement Results, VISIT http://bit.ly/2zplXkf

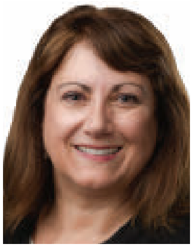
At Ohio State, Patton's team uses a formal follow-up review process for all recommendations that are included in the final report. The first phase is to follow up with clients every 90 to 120 days until the recommendations are resolved. A follow-up review report is issued to the same distribution list that received the final report. After the second follow-up, any remaining unresolved findings are escalated to senior university leadership for consideration and prioritizing with the unit. In fact, according to Patton, during the second follow-up review, the senior leader is responsible for obtaining an updated management response and resolution time frame to set the priority for the unit. If, after a third follow-up review, any unresolved comments remain, Patton discusses those in detail with the audit and compliance committee.

But there is another possibility as well. Management may decide to accept the risk and not resolve the comments. These situations also are elevated to the audit and compliance committee for discussion. Patton notes, "Of course we hope it doesn't get to that point. And it rarely does for us."

Principal Financial Group's process for follow-up is similar to that of Ohio State, with progress checks quarterly. Bolton explains that recommendations are rated critical, high, moderate, and low. Anything moderate or higher receives additional testing to make sure it is implemented to internal audit's satisfaction. Low items are not tested as vigorously: "We accept their word it's done." A quarterly report on the percentage completed and the status of follow-up items is issued to senior management and the audit committee.

UNDERSTAND THE REASON

Alvero points out the need to determine the reason for nonimplementation. Did management make a business decision, choosing not to take the recommended action based on the risk to business objectives balanced against other factors, such as cost and resources? Or did management simply ignore the recommendation?



"We accept their word it's done [when dealing with low-rated recommendations]."

Cindy Bolton

"Making a business decision not to implement a recommendation is not necessarily a red flag," he says. "It is not the same as ignoring a recommendation, which obviously would be a concern." Investigation may be needed into the extent of the refusal to implement, because that is generally not a one-unit decision. In many companies, the business office, the CRO, the audit committee, and other individuals or groups, depending on organizational structure, would have to support the decision.

In some cases, limited resources within the internal audit department may affect follow-up efforts. In these cases, Hersh advises internal audit to prioritize the key risks and then focus on implementation of corrective actions for the more significant risks. He considers this necessary when assessing whether management has inappropriately accepted a risk, in internal audit's opinion, by not implementing corrective actions.

WORKING TOWARD ONE GOAL

Ultimately, as with so many business transactions, *what* is being done is often secondary to *how* it is being done. For its recommendations to carry weight and earn full consideration, internal audit must act as a trusted advisor to the business, establishing and demonstrating a mindset of cooperation and collaboration, not an adversarial relationship. As Bolton puts it, "We have different units, different priorities, different purposes, but ultimately we are one company. We are all working together, trying to do the right thing." Ia

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

ANGELO LANO / SHUTTERSTOCK.COM

By uncovering significant mistakes and fraud, auditors can better illustrate the impact of a failed control.

Christopher Kelly

The Dollar Value *of* Error-seeking Audits

Attention to the risk of significant errors and fraud is a recurring theme throughout The IIA's International Professional Practices Framework. For example, under mandatory Attribute Standard 1220.A1, internal auditors must exercise due professional care by considering the "probability of significant errors, fraud, or noncompliance."

In the public and private sectors, errors that slip through normal business cycles are likely unintentional. *Fraud* is defined in the Standards Glossary as, "Any illegal act characterized by deceit, concealment, or violation of trust" and therefore entails intentionality on the part of the wrongdoer. The dichotomy between what is an unintentional error and what is an intentional fraud may not always be clear cut.

Some audit methods seem better suited to finding errors and fraud than others. Audit methods that rely on representations by management, and by which auditors gain confirmation that controls have operated as intended—such as interviews, control self-assessment checklists, walk-through tests, transaction sampling, and analytical review of reasonableness—can be vulnerable to confirmation bias. Such conclusions could be uncontroversial, but risk internal audit's reputation if significant errors or fraud come to light at a later date.

Error and fraud can be further obscured by insufficiently negotiated remedial actions at closing meetings with audit clients (see "When Recommendations Go Unaddressed" on page 48). Experience over many years suggests the timely completion of agreed-on actions sometimes linger unfinished, or are implemented less diligently than what internal audit intended. It follows that confirmation bias in fieldwork, combined with under-negotiated and then poorly implemented remedial actions, can conspire to hide the possible existence of significant errors and fraud, which occur more frequently than might be expected. One way to minimize the risk of providing false assurance and boost internal audit's value to the board is to search for the very errors internal controls are intended to prevent.

Search for the very errors internal controls are intended to prevent.

LOOKING FOR ERRORS

Pursuing significant error and fraud requires hypothesizing about what potentially could occur. Ideally, this is done by harnessing multi-industry experience and creative thinking—starting with the worst conceivable scenarios—and then planning audit fieldwork with the foreknowledge that actual findings may differ from what was hypothesized.

Error detection methods include:

- Cross-matching data that is not normally matched, such as cell phone metadata and building access data.
- Using data mining.
- Using Benford's Law to highlight unusual transaction deviations.
- Interrogating email content.
- Listening to personnel who may be willing to divulge information about how controls have been bypassed.

Internal audit has an edge in that it normally has data mining tools at its fingertips; a network of trusted contacts across the organization who can be valuable sources of information; and a wide view of end-to-end processes; whereas, many employees are limited to the restricted perspective of their own department. By leveraging these advantages, internal audit can see what may be invisible to others.

It is easier to persuade management of the impact of a weak control if an actual error with a quantifiable impact is found as compared to surmising about an unproven control failure with the potential to cause a negative financial impact. Internal audit has a strong argument for process improvement and management has a weakened defense if an actual error or multiple errors are tabled for discussion at the closing meeting.

Through hypothesizing error and fraud scenarios in our audit planning across various organizations, my internal audit team has been able to boost its reputation for findings that translated into fast management responses, material dollar recoveries, and, in more than a few cases, personnel changes that were long overdue.

Case No. 1. By seeking deposit limit exceedances, internal audit found £75 million (US$99 million) in treasury deposits at a British infrastructure services company intended to maximize bank interest, but that significantly

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

exceeded board-approved deposit limits with those financial institutions. Management had elevated its own self-interest in maximizing revenue-based personal bonuses while circumventing the board's risk appetite. Management self-interest has been a frequently observed bias that has come to light in error-seeking audits.

Case No. 2. Internal auditors found AU$60 million (US$47 million) in a single bank account at an Australian transport company earning zero interest, owing to management's inattention to value-for-money. The board agreed the money should have been invested at low risk across several institutions for interest earnings of at least AU$900,000 (US$705,000) per year. In both Case No. 1 and Case No. 2, the lack of a treasury report concealed from the board how funds in treasury were stewarded, resulting in the discovery of material cash held in the wrong places.

Case No. 3. By constructing numerous error hypotheses before and during fieldwork, internal audit found £8 million (US$10.5 million) in erroneous overcharges by maintenance subcontractors of a British engineering company. There were approximately 50 separate error and fraud findings hidden in aggregated lump-sum claims for payment that client management had signed off with inadequate due diligence checks before payment approval. Although multiple management sign-offs had occurred up to the CEO, each had assumed the manager below had performed detailed checks on the subcontractor charges. Once internal audit quantified the overcharges, nearly all were recoverable without any need for lawyers. A surprise dividend arising from this audit was that when the engineering company's CEO was subsequently promoted to a more senior CEO position at a larger firm, he took the chief audit executive (CAE) with him.

Case No. 4. When reviewing the general ledger for unmanaged assets, £4 million (US$5.3 million) in overdue, uncollected debt was found at the British subsidiary of a U.S. parent company. The debt had escaped credit control's attention as it was from nonroutine customers that fell outside normal business, therefore bypassing routine debtors reporting. Yet 50 percent remained collectible, resulting in a £2 million (US$2.6 million) windfall cash inflow and a cleaner balance sheet.

Case No. 5. Accounts payable had failed to detect AU$2 million (US$1.6 million) in duplicate payments to suppliers across different clients in retail, transportation, government, and engineering. Although the accounts payable systems were capable of detecting the duplicates before payment, unbeknownst to senior management, those system warnings had been switched off or were ignored by local supervisors. Internal audit used its knowledge of the controls that should have been in place to independently perform data mining checks specifically targeting undetected duplicates. To our surprise, dozens were found. Management recovered the overpaid amounts from the suppliers and switched back on the inbuilt accounts payable system controls.

Case No. 6. Internal auditors uncovered AU$1 million (US$788,000) in fraudulent sick leave and unrecorded annual leave by employees of an Australian transport company by hypothesizing that vacation fraud was possible and seeking errors through cross-matching payroll data to cell phone usage, vehicle usage, and building entry data. At first, management tried to argue that internal audit had breached privacy regulations by analyzing the whereabouts of employees. But the CAE proved that use of the organization's own telecommunications metadata to investigate employee whereabouts during work hours was allowable under local privacy regulations. The audit concluded not only that employee culture was in need of repair, but also that the supervisory culture was abysmal, resulting in several management changes. This impacted favorably on workforce productivity, balance sheet leave liabilities, and overtime costs, which had been incurred as a direct result of employees taking false leave over many years.

Management self-interest has been a frequently observed bias.

Case No. 7. In a case reflecting significant error and fraud, internal audit found motor vehicle usage policies that were poorly written and weakly applied at two separate companies. Moreover, the outside leasing companies had stacked risks and rewards of lease charges in their own favor. As a result, motor vehicles were being used fraudulently for nonbusiness purposes, the parent organizations were unaware of driver license cancellations because of nonexistent driver declarations, vehicle accident rates were worsening with consequent increases in insurance premiums because of unchecked driving records, and the leasing companies were

Advertisement

AUDITOR SPOTLIGHT

CaseWare Analytics recently had the opportunity to speak with Marcelo Barreto Rodrigues (IM), Rear Admiral and General Director of Internal Control Center of Brazil's Navy, to discuss the Navy's use of data analytics. Here's some of the reasons why he's an advocate for data analysis tools.

Q: Why did your organization get started with data analysis software?

A: We first adopted data analytics to facilitate auditing at the Internal Control Center. We knew that it was preferable to traditional auditing for many reasons, including:

- Reduced time and travel costs for audits
- More frequent audits
- Faster reporting of results, allowing timely action to be taken
- Reinforced control environments, which dissuades reprehensible actions, unproductiveness and carelessness at work

Q: Why was CaseWare IDEA your data analysis software of choice?

A: My coworker was familiar with the software and knew it had been successful in other governmental agencies. Plus there are many benefits to using IDEA, including that it can import virtually any type of file, such as text files, reports in text or PDF format, Excel and other databases. It also has functions specifically for auditors, including join, comparison, summarization and data stratification.

IDEA is very easy to navigate, especially when it's necessary to create several secondary databases from a main database. It's great too that users don't need to have specific knowledge of databases to do this.

Q: What are some interesting things you can do with your data analytics tool?

A: We can cross reference and compare data saved in different Navy systems, both internal and external, to identify irregular or duplicate payments, for example. We can also verify present facts, make timely corrections, and perform preventive fiscal inspections—online and on time.

Q: How did data analysis software affect your audits?

A: It changed the dynamics of our audit processes, which were previously performed through manual reconciliations. Now they are automated through conciliations of the databases of the Brazilian Navy and other agencies of the federal government.

Q: How do you convince others to use data analysis software?

A: By simply presenting the results obtained from using the tool. I've already suggested to other military organizations that they should use a data analysis solution that improves the effectiveness of control processes. We also share our successes in continuous auditing with the Internal Control Centers of the other Armed Forces, showing how much time and costs for audits can be reduced.

To learn how CaseWare IDEA can help make your audits more effective, visit www.casewareanalytics.com.

CaseWare Analytics

Almost 30% of fraud cases identified by researchers were preceded by reports of material weakness in internal controls, according to Internal Control Weaknesses and Financial Reporting Fraud.

charging unwarranted end-of-lease penalties. Although the companies could not recover past costs, they each avoided AU$1 million (US$780,000) in annual future costs through policy and control improvements resulting from the audit.

Case No. 8. Sometimes error and fraud come to light through internal audit's network of contacts. A vague but critical tip-off from a concerned staff member disclosed that the chief financial officer (CFO) shared proprietary board information with an IT firm bidding on multimillion-dollar contracts, and that the CFO was a director and shareholder of that IT firm. Audit confirmed the related-party connection with the securities regulator, and then used its charter access rights to study the CFO's emails and cell phone records to verify the passing of proprietary information. In doing so, new, unexpected wrongdoings also came to light. The company terminated the CFO, fixed its conflict of interest procedure, recovered some historic costs, and stopped multimillion-dollar future overspend.

These cases illustrate the diversity of policy, risk management, system, procedural, and contractual failings that are discoverable through seeking significant errors and fraud when planning and executing audits.

COMPELLING EVIDENCE

Appreciation of internal audit's role and reputation as the board's champion improved noticeably across the organizations when hard-to-dispute evidence of material error was tabled for discussion. Remedial actions followed quickly. Often, before the audit report was issued, controls were improved, costs were recovered, future costs were avoided, and—in the worst cases—offenders moved on.

Boards prefer it when errors are discovered early through internal audit's error-seeking vigilance rather than after the event by public whistleblowing, external audit, regulators, or the media. Even if an error-seeking methodology finds no wrongdoing, that in itself is a strong, albeit not absolute, form of assurance on the effectiveness of controls.

CHRISTOPHER KELLY, DPROF, FCA, MIIA, *is a partner with Kelly & Yang in Melbourne, Australia.*

STATEMENT OF OWNERSHIP, MANAGEMENT, & CIRCULATION

Extent and Nature of Circulation	**Average No. Copies** (October 2016- August 2017)	**Actual No. Copies** (August 2017)
Total Number of Copies	79,687	78,290
Paid Circulation Mailed Outside-County Paid Subscription	58,909	58,612
Paid Distribution Outside the Mails Including Sales, Through Dealers and Carriers, Street Vendors, Counter Sales, and Other Paid Distribution Outside USPS	18,836	16,290
Total Paid Distribution	77,746	74,902
Free or Nominal Rate Copies Mailed at Other Classes Through the USPS	67	85
Free or Nominal Rate Distribution Outside the Mail (*Carriers or other means*)	630	470
Total Free or Nominal Rate Distribution	697	555
Total Distribution	78,442	75,457
Copies Not Distributed	555	865
Total	78,997	76,322
Percent Paid	99.11%	99.26%
Paid Electronic Copies	15	24
Total Paid Print Copies + Paid Electronic Copies	77,761	74,926
Total Print Distribution + Paid Electronic Copies	78,457	75,481
Percent Paid – Both Print & Electronic Copies	99.11%	99.26%

Publication Title: *Internal Auditor*

Publication Number: 0020-5745

Filing Date: 10/25/17

Issue Frequency: Bi-monthly

Number of Issues Published Annually: 6

Annual Subscription Price: $75.00

Mailing Address of Known Office of Publication: 1035 Greenwood Blvd., Suite 401, Lake Mary, FL 32746

Address of Headquarters: The Institute of Internal Auditors, 1035 Greenwood Blvd., Suite 401, Lake Mary, FL 32746

Contact Person: Gretchen Gorfine
Telephone: 407-937-1232

Publisher: Monica Griffin, Sr. VP, CMO, The Institute of Internal Auditors, 1035 Greenwood Blvd., Suite 401, Lake Mary, FL 32746

Editor: Anne Millage, Editor-in-chief, The Institute of Internal Auditors, 1035 Greenwood Blvd., Suite 401, Lake Mary, FL 32746

Managing Editor: David Salierno, The Institute of Internal Auditors, 1035 Greenwood Blvd., Suite 401, Lake Mary, FL 32746

Owner: The Institute of Internal Auditors, Inc., 1035 Greenwood Blvd., Suite 401, Lake Mary, FL 32746

Issue Date for Circulation Data: October 2016 - August 2017 / August 2017

Signature and Title: Gretchen Gorfine, Production Manager, 10-25-17

BY LANE KIMBROUGH EDITED BY KAYLA FLANDERS

STRUCTURED FOR STRENGTH

Creating a center of excellence can enable a capable first line of defense.

Audit, compliance, and risk functions have always emphasized first line of defense ownership of risk management and controls. Yet audit professionals routinely encounter clients who lack a basic understanding of controls for managing risks. How pervasive is this condition, and should senior management and the board be concerned? A formal review of the first line's risk and control capabilities may identify some significant findings:

- Lack of clear accountability for developing and sustaining risk and control proficiency across the first line.
- Insufficient knowledge and skills among first line personnel regarding control design and risk management fundamentals.
- Nonexistent monitoring of first line control design competence.
- Inadequate integration of risk and control disciplines within management activities.

If such potential findings ring true for your organization, I recommend establishing a function that is fully devoted to, and accountable for, closing these gaps and maintaining a capable first line. This first line center of excellence (CoE) is primarily responsible for demonstrably improving the risk and control capabilities and performance of the first line of defense across all organizational units.

Services and deliverables provided by the CoE go beyond training and awareness to include risk management tools, best practice sharing, risk and control advisement, and collaboration with the second and third lines of defense on matters of common interest. Suitably positioned, the CoE could influence management activities, performance incentive mechanisms, and operations methodologies to integrate sound risk management and control design into the organizational culture.

The CoE should be staffed with a small team of professionals who have strong working relationships across business units and all lines of defense. Their qualifications should include an understanding of a broad range of disciplines used by the organization, and how these disciplines map to risk and control frameworks. Skills and experience in internal consulting, change management, and developing training and tools also are desirable, supported by the ability to lead, collaborate, and influence to overcome obstacles.

Where should this team reside within the organization? Let's look for a home in each of the lines of defense.

Third Line – Internal Audit – Functions That Provide Independent Assurance While audit shops have expertise in risk and control, and audit

READ MORE ON GOVERNANCE Visit InternalAuditor.org/governance

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

fieldwork provides insights into control weakness themes across the enterprise, internal audit is not chartered to equip the first line. Audit teams need to maintain their independence, and their primary focus is completion of the audit plan to enable relevant reporting to senior management and the board. Advisement to the first line is a secondary role, and accountability for enabling first line capabilities would be an awkward fit within the third line.

Second Line – Specialty Risk and Compliance Groups – Functions That Oversee Risk These functions likewise have expertise in risk and control, but their focus is on specialty areas such as financial control, security, fraud, quality, risk quantification, and compliance. Though enterprise risk management departments sometimes provide first line training and advisement, these services are subordinate to their risk oversight obligations, such as standards, risk aggregation, and reporting. As oversight units, second line functions are commonly perceived by the first line as enforcers of requirements rather than enablers, reflecting the natural tension between overseers and the overseen.

First Line – Business Operations – Functions That Own and Manage Risks Personnel across the first line are, by definition, embedded in the business and thus closest to the action. They take and manage risks constantly. They design, redesign, and execute controls daily. However, there are generally only limited pockets of risk and control proficiency, and the typical first line professional has little exposure to control design and risk management training or advice. Given the expectation that the first line excel in owning and managing risk, it appears this would be the most logical place to insert the CoE.

Many organizations have precedents for CoEs within the first line, such as specialty units devoted to project management, data analytics, or supplier management. A CoE dedicated to the first line's fundamental control and risk management responsibilities, positioned within the first line, itself, would be a natural fit. It would provide first line process owners and management an unintimidating place to go to for risk and control expertise, advice, and best practices.

The pluses for the first line are clear: improved design of control environments, stronger risk management, and smarter risk taking, leading to more effective operations and increased likelihood of achieving business objectives. Moreover, an effective CoE fosters stronger ownership of risk and control where it belongs.

The second line benefits by having to spend less energy cultivating the first line, thereby enabling stronger second line concentration on its oversight mandate and risk specialties. A proficient first line also will contribute to more positive messaging in the second line's oversight reports, reflecting a more effective first line and an improved risk management culture.

The third line can enhance its assurance that the first line is committed to excellence in risk management. The CoE, itself, is an auditable entity and should be regularly reviewed as such, along with its impact on the organization's risk maturity.

Senior management can leverage the existence and effectiveness of the CoE to tangibly illustrate dedication to proactive management of risk across the organization. This may be especially beneficial in highly regulated industries, as external auditors and regulatory examiners are likely to be interested in how the CoE approach improves risk diligence and operational compliance.

The organization as a whole benefits by enabling lines of defense functions to focus more fully on their primary and distinct responsibilities. This approach also improves the risk culture by enabling a healthy balance between proactive risk management through capable control design, and reactive identification of issues that need fixing.

As a key advocate for effective risk management and controls, internal audit can wield its influence with senior management and the board in support of the CoE. To bolster this business case, audit may conduct a root-cause analysis pointing to a lack of controls understanding as a key contributor to weaknesses across the enterprise. Internal audit can highlight the dangers of not having a risk and control savvy first line, and play a part in holding the CoE accountable for embedding risk and control know-how across operations.

Internal audit also may collaborate with the second line of defense to analyze repositories of audit reports, reviews, and assessments to distill control weakness themes and best practice recommendations. These would be combined with lessons learned by the first line, itself, and disseminated by the CoE to help process owners and managers avoid similar problems.

Judicious risk takers and control designers don't happen by accident, and they warrant a targeted investment. But the promise of an effective CoE goes well beyond reducing the number of disconcerting interactions with clients who don't understand risk and control. The entire organization stands to gain as improvements in business results arise from a risk culture characterized by pervasive control capabilities. Ia

LANE KIMBROUGH, PHD, CIA, CRMA, CCSA, *is director, business risk and controls, at USAA in San Antonio.*

Internal Audit, Risk, Business & Technology Consulting

Navigating the Complexities of Corporate Culture

Internal Auditing Around the World, *Volume XIII*

Culture audits are an opportunity for auditors to talk to employees, managers, customers and vendors, and report on whether the company is living its values, or whether they are hollow. Read more from 15 audit leaders featured in this publication.

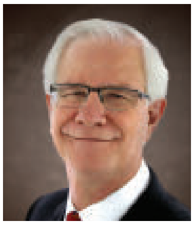
Download a copy at protiviti.com/iaworld.

protiviti®

Face the Future with Confidence

© 2017 Protiviti Inc. An Equal Opportunity Employer M/F/Disability/Veterans. PRO-1017

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



BY J. MICHAEL JACKA

A CIRCLE OF ADVOCATES

Internal audit's value is often best conveyed by the clients it serves.

Internal auditors spend a lot of time trying to convert people. In some cases, the conversions are small: "Here are the findings—let's come to agreement on what is wrong and how to make it better." In other cases, the conversions are much larger: "In spite of what you think, internal audit is not here to bayonet your wounded; we're here to help the organization achieve its objectives." When we do that job well, we build a circle of advocates who become our best promoters.

We talk a lot about how to make those conversions—how to sell internal audit to the naysayers who see us as the enemy. And honing that sales pitch is important, as many clients will respond well to our efforts. But we seldom discuss when we should stop selling and just simply walk away.

The nasty truth is that some people will never buy what internal audit sells. They have been burned, they have their own agendas, or they just refuse to see internal audit as an ally. And as the old saying goes, never try to teach a pig to sing; it wastes your time and it annoys the pig. Internal auditors must recognize that some clients, no matter how much we try to convince them, will never sing the praises of internal audit. And once we have identified them, we must be willing to walk away.

Of course, ours is a risk-based approach, and if the risks lie within the purview of someone who just doesn't like us, we can't abandon the person, department, or organization. No, even in the face of dislike and even pure hatred, we must still do our work, maintain our standards, and continue to move forward. But that doesn't mean we should waste additional effort trying to convince the client of our added value.

Keep in mind that, even when we "give up" on such clients, we are still selling ourselves to them. First, by continually providing value, we keep chipping away at the wall they have erected between their department and ours.

But a more important sales job—and the more convincing one—comes from that circle of advocates. Redirecting our efforts away from those advocates as we try to sell to the naysayers can begin eroding our fan base. But if we maintain our focus on those fans, they become stronger advocates. And the word will start to get around. And soon enough the naysayers will hear their co-workers praise internal audit as a group that provides value, is a trusted advisor, and represents a real partner to the business.

Tom Peters (as he so often does) put it best: "Greatest waste of time? Trying to 'convert' non-believers. Instead, surround 'em. That is, you don't 'convert.' 'They' 'discover'—come to appreciate what you're doing because a couple of *their* pals have joined up." When it comes to selling internal audit, sometimes the client's voice speaks the loudest. 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

SUCCESS FACTORS

The IIA's global and North American board chairs share what internal auditors need to succeed in 2018.

J. MICHAEL PEPPERS, CIA, CRMA, QIAL
Chairman
IIA Global Board

SHANNON URBAN, CIA, CRMA
Chairman
IIA North American Board

How can internal audit better align with the organization's strategic priorities?

PEPPERS All of The IIA's recent stakeholder surveys tell us we must maintain or enhance organizational alignment to stay relevant. A practical test to ensure internal audit has the right balance is to consider how much of its risk assessment efforts are spent looking backward at past events versus looking forward at what is to come. Confirm that assurance and advisory engagements are selected to address the current objectives of the organization. Of course, that assumes you are knowledgeable about those strategic activities.

URBAN We are in a transformative age—business today is anything but usual. Strategic priorities are driving organizations more than ever to continue to protect and grow. This is where we can add tremendous value by tying our audit plans back to the organization's strategy. If our assurance and consulting work is not aligned with what's most important to the organization, we should challenge why we are doing it. If it's a regulatory or management requirement, then we should identify ways to cover those areas more efficiently so we can focus more on the risks aligned to strategic priorities.

How should internal audit adapt to meet changing expectations?

URBAN It is critical that internal audit practices and processes are flexible and able to adapt to the disruptive changes happening around us. Many internal audit functions follow prescribed practices that are carved in stone in the audit manual. This helps with consistency and quality, but it sometimes keeps auditors from exploring alternate approaches that may be more impactful or efficient for a particular risk area. Internal auditors should allocate time during the planning phase of an audit project to challenge themselves on the approach and techniques they deploy, and make innovation or continuous improvement part of the planning process.

PEPPERS We have to be in touch with those expectations. Our audit team members are the best resources to help with that. They should be encouraged to listen to our customers and come back and tell us what they hear. As a group, we can then be responsive. While adaptation and evolution are imperative, there are also fundamental principles and practices that shouldn't fluctuate wildly. So thoughtfully consider where and when to invest time and resources into change.

What will be the impact of disruptors like data analytics, artificial intelligence (AI), and blockchain?

PEPPERS I find it telling that some internal auditors still consider data analytics to be a new or recent disruptor.

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

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

We've had that technology available to us for more than 20 years, and some still don't even touch it. When we think of how AI will impact our organizations in the next few years, auditors who take a similar hands-off approach will do so at their own peril. We want to be in a future position to audit these emerging technologies, so we need to be around the table as the related governance, architecture, and infrastructure decisions are being made.

URBAN These emerging technologies are disrupting long-held business norms, processes, and models. They hold the key for many organizations to drive more cost effective and reliable operations, but may be introducing risks no one has yet thought about. They also promise incredible new capabilities for auditors who understand and adopt what these new enablers can bring to the audit process. I like to think about these technologies as multipliers of audit capacity and capability—if we are brave enough to take the leap.

How can CAEs improve their relationships with the board and audit committee?

URBAN A lot of it comes down to better communication and building trust. It's easy to assume we know what our stakeholders want, or need, from internal audit—but very few of us ask directly. In our organization, we touch base with key stakeholders at least once a quarter, and not just about the status of the plan or other administrative matters. We talk about what's important to them as stakeholders, and what defines a high-quality and high-value audit service. How are we doing, and where are we missing the mark? We try to understand their personal and social style, their communication preferences, etc.

PEPPERS I think a CAE has to start by candidly acknowledging the current state of those relationships. Don't just assume all is well. A great indicator is the frequency of communication and who initiates it. Solicit sincere feedback about style and then either maintain or modify accordingly. It also is imperative that CAEs take full advantage of every opportunity they have in front of their audit committees and boards. We must creatively and effectively represent to them the full spectrum of our work and the impact we are making.

How can internal audit add value to the organization's sustainability strategy?

PEPPERS Auditors need to have a holistic, long-term view of the organization, its objectives, and its risks. This includes issues around its long-term sustainability and the resources it uses to deliver products and services to its consumers. For example, many audits focus on the process, and while many auditors may use a process mapping effort known as SIPOC [Suppliers, Inputs, Process, Outputs, and Consumers], typically not much time is spent understanding the risks associated with the supplies and inputs into the process. Who is providing the inputs? Where do they get their supply? Is there limited capacity of the supplies, or does demand outstrip supply? What would happen if that supplier could no longer deliver? This is just one path of questioning that opens up by simply looking beyond what is normally audited. There are many other possible pathways when operations are considered from a longer-term, sustainability perspective.

URBAN According to the Center for Board Matters' 2017 Proxy Season Review, fully 49 percent of all shareholder proposals are related to environmental or social issues. With such diverse topics as greenhouse gas emissions, board diversity, and environmental health and safety, many internal audit teams are finding a place for these topics in the audit plan. Internal audit can address sustainability and environmental, social, and governance issues in many ways. One way is to look at the overall governance structure of sustainability. Is it a stand-alone function that issues a report once a year, or is it integrated into the business? Does it measure and report on key metrics and have reduction targets in place? Is it led by a senior executive? Some organizations also are examining whether and how to integrate nonfinancial risk into their overall enterprise risk management process, especially in light of recent U.S. Securities and Exchange Commission and shareholder interest in these areas.

How does internal audit attract and retain the right type of talent considering these issues?

URBAN Talk about disruption! The entire business model for how candidates are sourced and from where they are sourced is changing across business. Internal audit is no exception. Organizations like ours are diving deeper into the universities to identify high-performing talent as early as freshman year to join our staff ranks. Traditional backgrounds and majors are still needed, but we are recruiting more data scientists, engineers, IT majors, and other non-accountants. Organizations are continuing to develop rotational leadership development programs that involve time in internal audit, but with the goal of building future business leaders—not future auditors.

PEPPERS Selection of the right team resources starts with a clear understanding by all of what the job entails. That clarity will increase the likelihood of the right match for the position, and job satisfaction will follow and improve retention. But that is increasingly more challenging given the dynamic nature of the environment we've been discussing. A CAE colleague recently told me she has totally revamped her recruiting to heavily weight critical thinking skills. When those are present, she finds the individuals are better able to perform, contribute, and grow over time. When that happens throughout the internal audit activity, everyone benefits. Ia

CIA
Certified Internal Auditor®

Drive Your Career Forward

IIA Certifications and Qualifications

Solidify Your Credibility.

Adding the Certified Internal Auditor® (CIA®) credential to your resume, LinkedIn profile, and business card will help you stand out and demonstrate you are:

- A true expert who understands and can apply The IIA's *Standards*.
- A stronger, more competent professional.
- Equipped for career-advancing opportunities.
- A credible and trusted internal auditor.

Becoming a CIA helps you build a stronger foundation to meet the present and future challenges you face in your career.

If you are looking to grow professionally, earning the CIA is an essential step.

Apply today at
www.theiia.org/CIA.

The Institute of Internal Auditors

IIA Calendar

IIA CONFERENCES

www.theiia.org/conferences

2018

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

MARCH 15
Environmental, Health & Safety Exchange
Aria Resort & Casino
Las Vegas

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

IIA TRAINING

www.theiia.org/training

DEC. 4–13
Fundamentals of IT Auditing
Online

DEC. 5–8
Various Courses
New York

DEC. 5–8
Various Courses
Denver

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

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

DEC. 11–14
Various Courses
Orlando

DEC. 12–15
Various Courses
Austin

DEC. 18
Fundamentals of Internal Auditing
Online

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

2018

JAN. 8–26
CIA Learning System Comprehensive Instructor-led Course – Part 1
Online

JAN. 16–18
Risk-based Auditing: A Value-add Proposition
Online

JAN. 16–25
Auditing Security Monitoring
Online

JAN. 16–25
Operational Auditing: Influencing Positive Change
Online

JAN. 22–31
Audit Report Writing
Online

FEB. 5–14
Assessing Risk: Ensuring Internal Audit's Value
Online

FEB. 5–14
Performing an Effective Quality Assessment
Online

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

FEB. 13–16
Various Courses
Phoenix

FEB. 13–22
Cybersecurity Auditing in an Unsecure World
Online

FEB. 19–22
Statistical Sampling for Internal Auditors
Online

FEB. 19–29
Fundamentals of IT Auditing
Online

FEB. 26–MARCH 1
Vision University
Orlando

FEB. 27
Fundamentals of Internal Auditing
Online

BER/JANUARY/FEBR

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 mark.ledman@theiia.org

BY MARK LEDMAN

ARE YOU AUDITING BY EMAIL?

Client interaction should never be confined to laptops and servers.

Technology has expanded internal audit's reach considerably in recent years. With the advent of sophisticated analysis and communication tools, practitioners can now gather and examine data without ever leaving the comfort of their office—a process sometimes referred to as "auditing by email." But internal audit needs to be careful with technology, despite its convenience and capabilities, ensuring the tools do not lead to a cessation of fieldwork. Auditors who hide away in their offices and perform work from afar risk missing potentially key insights and communication opportunities.

In the past, nearly all operational engagements required physical visits to examine source documentation. Site walkthroughs and client face time were assumed—in fact, on-site activity often comprised a large proportion of engagement schedules. Today, many auditors can extract transactional data directly from enterprise resource planning systems and get all the information they need remotely. The transition to electronic data has made retrieval of original documents a less time-consuming and arduous process.

Nonetheless, internal auditors need to ensure the technology does not, in some ways, work against them. Communication is key, and it is more likely to occur regularly with internal audit staff available on-site. Ongoing communication helps the audit team understand the client's business, build relationships, and improve the design of audit procedures. Plus, it reduces the possibility of blindsiding clients with unexpected news.

Removing client interaction and physical presence on engagements can deprive internal audit of potentially valuable information. Without the auditors' eyes and ears on site, it can be much more difficult to obtain sufficient understanding of the internal control environment or help identify key risks that may threaten organizational success. The lack of presence also presents a challenge to consulting work, making the role of trusted advisor difficult to achieve.

Spending time on-site allows the audit team to better tailor its work to individual circumstances. When practitioners move through the organization and physically observe the client's environment, they can adjust the audit program more easily as new information becomes known. These adjustments, in turn, provide greater value to the client, and to the organization as a whole.

High-performing businesses need to stay focused on customers and their needs. By the same token, high-performing audit functions must be attuned to the needs of stakeholders—a task often best accomplished in person. Practitioners should avoid relinquishing their client interactions to technology and remember that the audit process is as much about building relationships as it is about individual effort. Great auditors not only excel at analysis and assessments—they also know when to close their laptops and step out into the real world. Ia

MARK LEDMAN, CISA, *is assistant state audit manager, North Carolina Office of the State Auditor, in Raleigh.*

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

Achieve exam day excellence with The IIA's CIA Learning System®

- **Comprehensive materials** teach the entire CIA exam syllabus and align with the 2017 IPPF®.
- **Mobile-optimized study tools** make it easy to study where you want and when you have time.
- **Flexible course options** allow you to study your way: self-study or online or in-person facilitator-led courses.

For more information or to try 10 free practice questions, **visit www.LearnCIA.com.**

The Institute of Internal Auditors

2017-0019-CIALS

Wolters Kluwer

TeamMate+

Proud to be recognized with the

GRC User Experience Award in Audit Management

Learn more about why TeamMate was chosen at
www.TeamMateSolutions.com/award

Copyright © 2017 Wolters Kluwer Financial Services, Inc. All rights reserved. 10235