Ia
INTERNAL AUDITOR
JUNE 2016
INTERNALAUDITOR.ORG

Analytics for All

N.A. Board Chair Advises Auditors to Craft Their Role

Assessing Anti-corruption Programs

IIA Conference Keynoters Address Emerging Risks

THE TOXIC LEADER

Internal auditors should be on the lookout for damaging leadership styles that can create an unhealthy corporate culture.

CELEBRATING 75 YEARS OF THE IIA

Ia
INTERNAL AUDITOR

JUNE 2016 VOLUME LXXIII: III

FEATURES

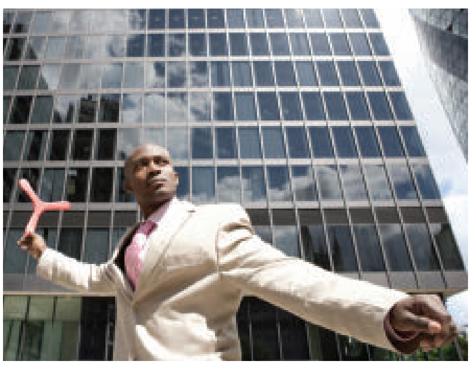
CELEBRATING 75 YEARS OF THE IIA

Ia
INTERNAL AUDITOR

JUNE 2016 VOLUME LXXIII: III

DEPARTMENTS

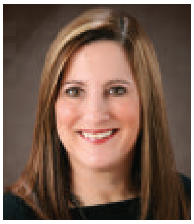
ONLINE InternalAuditor.org



Find us on Facebook

COVER: GARY HOVLAND
ILLUSTRATION: TOP, JAMES ENDICOTT / ILLUSTRATION SOURCE
PHOTO: BOTTOM, MJTH / SHUTTERSTOCK.COM

Internal Auditor ISSN 0020-5745 is published in February, April, June, August, October, and December. Yearly subscription rates: $75 in the United States and Canada, and $99 outside North America. No refunds on cancellations. Editorial and advertising office: 247 Maitland Ave., Altamonte Springs, FL 32701-4201, U.S.A. Copyright © 2016 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 Altamonte Springs, Fla., and additional offices. POSTMASTER: Please send form 3579 to: Internal Auditor, 247 Maitland Ave., Altamonte Springs, FL 32701-4201, U.S.A. CANADA POST INTERNATIONAL: Publications Mail (Canadian Distribution) Sales Agreement number: 545880; GST registration number: R124590001. Opinions expressed in *Internal Auditor* may differ from policies and official statements of The Institute of Internal Auditors and its committees and from opinions endorsed by authors' employers or the editor of this journal. *Internal Auditor* does not attest to the originality of authors' content.



WHEN TOXIC CULTURE HITS HOME

Toxic leaders create toxic workplaces. How do you know when your company's culture is toxic? If you do a Google search for "toxic workplace," you'll get numerous articles on the signs to look for. One sign shows up repeatedly in these articles: Your work negatively affects your health—physically and emotionally.

This subject hits home. Several years ago, my husband found what he believed to be his dream job: an accountant for a company in an industry he had grown up around and loved. For the first several years, everything was great—and then there was a change in management. The new executives had little interest in learning how the business worked, managed through fear and intimidation, and were big on hiring friends and family. Rumors ran rampant about restructuring and dismissals.

My husband would send me texts at least twice a week after being verbally assaulted by one of the new executives. He came home from work every night stressed and depressed. His blood pressure shot through the roof. So he did what he knew he needed to do—he got out. He was able to find a job in accounting in the same industry. He was lucky.

Not everyone is as fortunate. Many people stay on the job, feeling like they don't have a choice and hoping, if they just keep their heads down and avoid the gossip and politics, it will get better. Unfortunately, "this is nonsense," says Liz Ryan, CEO and founder of the Human Workplace, and author of "Six Signs Your Company's Culture is Toxic" (*Forbes*, August 2015). "In the history of mankind a broken corporate culture has never gotten better on its own. Your two choices are to leave the organization or to name the elephant on the table and let some air into the conversation."

Shining a light on the problem is never easy. Enter internal audit. As author Jane Seago points out in this month's cover story, "internal auditors must remain vigilant in spotting [toxic leaders] and taking appropriate steps to contain the damage (see "Toxic Leaders, Toxic Culture" on page 28). With the help of a team of IIA experts, Seago identifies several traits of toxic leaders and asks audit leaders and corporate culture experts their thoughts on internal audit's role in identifying these individuals and effective mitigation tactics.

From a business standpoint, toxic cultures affect an organization's productivity, company value, creativity, profitability, and growth and often are at the root of fraudulent behavior. From a personal standpoint, toxic cultures affect lives, both of the employee experiencing it and the family he or she goes home to. When a toxic culture can't or won't be changed, it's time to consider other employment options. No job is more important than one's health and happiness.

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.

Risky Payroll

"On the Hunt for Payroll Fraud" views payroll risk from an organizational savings and shareholder value standpoint instead of from a compliance with employee contract terms and conditions standpoint. Payroll departments should have continuous checks and balances to ensure risks of inappropriate and excessive payments are prevented, detected, and corrected timely.

OWAIS RIZVI *comments on Chris Kelly and Frans Deklepper's article, "On the Hunt for Payroll Fraud" (April 2016).*

Ethical Dilemma

I enjoyed reading your article. The United Way honor charity box was a brilliant idea. Whoever came up with this was a genius. There is no doubt that it touched the employees' soft spots and ended the ethical dilemma facing Axel Co. This reminds me of the old saying from Plato, "Good actions give strength to ourselves and inspire good actions in others."

MARILOU PARAYAOAN *comments on James Scott's article, "The Ticking Ethical Time Bomb" ("Fraud Findings," April 2016).*

Key Risks

Internal auditors should consider relying on risk management systems where available, taking into account their maturity level. I fully support internal audit making an effort to integrate its risk assessment with the one at the enterprise level, providing that enterprise risk management (ERM) has been reviewed and assessed as mature enough to be relied upon. Even then, necessary safeguards should be taken so internal auditors do not lose sight of those risks that relate directly to the existence and adequacy of the existing ERM system.

Another important aspect is that internal auditors have internal and external stakeholders with conflicting expectations and interest in their work. Stakeholders have a different perception of what constitutes a key risk to the organization. Consequently, internal auditors need to be aware of this and include the relevant risks in their own risk registers, which will form the basis of their annual audit plans.

TUNCAY EFENDIOGLU *comments on Dan Clayton's article "Collaborative Risk Management" ("Risk Watch," April 2016).*

Niche Position

Uncertainties and risks go hand in hand. The more complex the businesses are, the higher level of oversight and monitoring is needed to mitigate the risks. Internal audit is in a very niche position to test the complex system's design, efficiency, and effectiveness in its internal control system. Internal audit's independence and objectivity provide the board and senior management the confidence that the right risks are being considered and proposed strategy and business plans are being executed.

LIMEI LI *comments on Ted Doane's article, "Public Sector Innovation" ("In My Opinion," April 2016).*

Ia
INTERNAL AUDITOR
JUNE 2016
VOLUME LXXIII:III

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")

ON THE RISE

Who Are Internal Auditing's Future Leaders?

What defines an **extraordinary** internal auditor?

Innovation, integrity, knowledge, and passion, among other qualities. Do you know a high-performing internal auditor who possesses the traits to become tomorrow's thought leader? Acknowledge their dedication and nominate them today.

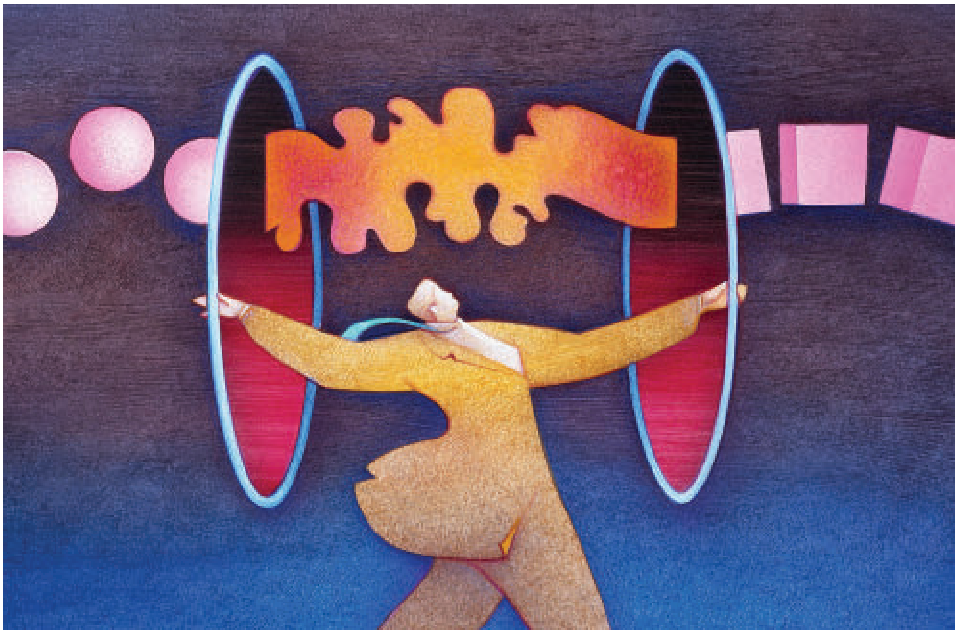
Internal Auditor magazine will recognize up-and-coming internal audit professionals in its annual "Emerging Leaders" article in December.

Nominate by June 30, 2016 at **www.theiia.org/emergingleaders.**

2016-0482

Survey says executives committed to uphill fight against corruption...
More organizations adopting cloud, but they don't fully trust it.

Update



BEST PRACTICE VS. REALITY

Attracting talent tops the strategic challenges boards face.

Boards of directors are taking on a "more strategic, dynamic, and responsive role" in their companies, according to the 2016 Global Board of Directors Survey from the WomenCorporateDirectors Foundation, search firm Spencer Stuart, independent researcher Deborah Bell, and researchers from Harvard Business School.

However, the report—which includes responses from more than 4,000 male and female directors from 60 countries—also shows "a gap between best practice and reality" in boards' ability to handle strategic challenges, especially related to talent issues.

For instance, though both public and private company directors rate attracting and retaining talent as a top challenge (38 percent and 48 percent, respectively) to achieving their companies' strategic objectives, respondents gave relatively low ratings to their own boards' talent issues such as board member diversity, human resources (HR)/talent management, CEO succession planning, and director evaluations.

"We do see in larger, more established public companies a greater maturity in their HR processes and deeper resources invested in talent management and development," says Julie Hembrock Daum, head

ENTERPRISE RISK INATTENTION

Risk oversight activities are not keeping pace with many organizations' high-risk business environments.

61% Report risks on an ad hoc basis.

30% Provide guidelines to management to assess a risk's probability and impact.

35% Do not formally assess emerging strategic, market, or industry risks.

54% Board review the top risk exposures facing the organization in a specific meeting.

Source: North Carolina State University ERM Initiative and American Institute of Certified Public Accountants, 2016 The State of Risk Oversight

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

IMAGES: TOP, JAMES ENDICOTT / ILLUSTRATION SOURCE
RIGHT, OLEKSANDR YUHLCHEK / SHUTTERSTOCK.COM

The IIA Congratulates the 2015 Certified Internal Auditor® (CIA®)* Award Winners!

William S. Smith Award – Gold
(Highest Scoring Candidate)
Michelle Hale, CIA *USA*

A.J. Hans Spoel Award – Silver
(2nd Highest Scoring Candidate)
Justin Swalberg, CIA *USA*

Kurt Riedener Award – Bronze
(3rd Highest Scoring Candidate)
William Flahr, CIA *USA*

Dr. Glenn E. Sumners Award – Student
(Highest Scoring Student Candidate)
Ashley Gervasi, CIA, CRMA *USA*

The IIA also recognizes the Certificate of Excellence (Next 10 Highest Scoring Individuals) and Certificate of Honor (Next 50 Highest Scoring Individuals) recipients:

Certificate of Excellence:*

Adriaan Borgermans, CIA, CFSA *Belgium*
Erick Cruz, CIA *USA*
Robert Cummings, CIA, CRMA *USA*
Philipp Christof Friebe, CIA *Switzerland*
Carmela Stephanie Hau, CIA *Philippines*
Naveed Khan, CIA *Saudi Arabia*
David Kingsland, CIA *USA*
Asim Kurt, CIA *Turkey*
Yatin Patel, CIA *Canada*
Jennifer Rue, CIA *USA*

Certificate of Honor:*

Jerome Afable, CIA *Philippines*
Brian Bench, CIA *Canada*
Akshay Bhat, CIA *UAE*
Man Wai Cheng, CIA *Singapore*
Pak Kei Andy Cheung, CIA *Hong Kong*
Brad Cooper, CIA *USA*
James Sherwin Credo, CIA *Philippines*
Scott Friedman, CIA *USA*
Benjamin Frost, CIA *USA*
Carson Guy, CIA, CRMA *USA*
Marie-France Hache, CIA *USA*
Michael Harrer, CIA *Austria*
Elizabeth Hogan, CIA *USA*
Michal Jedruszak, CIA *Poland*
Nikhil Khanduja, CIA *Canada*
FATMA KOCA, CIA *Turkey*
Sarah Kooistra, CIA *USA*
Amie Laufer, CIA *USA*
Marion Lespiau, CIA *GBR*
Fred Long, CIA, CRMA *USA*
Ilago Mabelya, CIA *Tanzania*
Timothy Marley, CIA *USA*
Alexandre Mayer, CIA *France*
Kelsey Messer, CIA, CRMA *USA*
Charles-Alexandre Moor, CIA *Ireland*
Case Mosby, CIA *USA*
Michael Murney, CIA *Canada*
Logan Musil, CIA *USA*
Akemi Nakanishi, CIA *Canada*
Michael P. O'Rourke, CIA *USA*
Dmitriy Osadchiy, CIA, CCSA *USA*
Edward Pasternak, CIA *USA*
Halldor Petursson, CIA *Iceland*
Marshall Phillips, CIA *USA*
Ryan Ralph, CIA *Canada*
Kashif Raza, CGAP *Pakistan*
Kristi Robertson, CIA *USA*
Luca Scalet, CIA *Italy*
Patrik Scheuber, CIA *Switzerland*
Christian Schiel, CIA *Germany*
John Schultz, CIA *USA*
Shalini Sellakumar, CIA *Canada*
Maarten Slotema, CIA *Netherlands*
Mark Spink, CIA *USA*
Mark Stanley, CIA, CRMA *USA*
Alfred Watts, CIA *USA*
Marcin Winiarczyk, CIA, CRMA *Denmark*
Marek Wronski, CIA *USA*
Syed Nayyar Raza Zaidi, CIA *GBR*
Zachary Zemenick, CIA, CRMA *USA*

Join with us in congratulating the following individuals for highest achievement on specialty certification exams.

Certification in Control Self-Assessment® (CCSA®)
Latif Cem Osken, CIA, CCSA *Turkey*

Certified Financial Services Auditor® (CFSA®)
Yaser Abdulla, CIA, CFSA *Bahrain*

Certified Government Audit Professional® (CGAP®)
Olivier Prigent, CIA, CGAP *Luxembourg*

Certification in Risk Management Assurance® (CRMA®)
Nathan Thomson, CIA, CRMA *Canada*

The IIA congratulates all 68 award winners. It is their dedication to their profession and understanding of the benefits and importance of certification that has led each to achieve these honors.

*Awards are based on individual performance on the core CIA exam parts 1, 2, and 3. With year-round testing, award recipients must pass each segment of the exam on their first attempt within one year of beginning the testing process.

of Spencer Stuart's North American Board Practice. "Many private companies, which tend to be smaller and have less brand awareness as a whole, often have less robust HR structures to attract the level of talent across the organization."

Other study findings call out gender differences, with female directors reporting higher levels of concern about risk than their male peers and more often favoring tools that foster board renewal, such as director retirement ages and term limits. Female respondents also are more likely to attribute the stagnant number of female directors to boards failing to make gender diversity a priority and to traditional, male-dominated professional networks, while male directors cite a "lack of female talent." A higher percentage of women support overall boardroom diversity quotas. **—S. STEFFEE**

BUSINESS LEADERS SUPPORT ENHANCED TRANSPARENCY

Executives recognize need to continue the fight against corruption.

Organizational leaders around the globe are calling for increased business transparency, according to EY's latest Global Fraud Survey. Escalating cybercrime, growing geopolitical tensions, heightened market volatility, and revelations from the Panama Papers, EY suggests, have ramped up pressure on companies to better manage fraud and corruption. More than 90 percent of respondents say they recognize the importance of establishing whether the activities of third-parties are legitimate.

Despite calls for transparency, results from the survey of nearly 3,000 senior business leaders from 62 countries and territories show corruption is still widespread. Nearly 40 percent of respondents say bribery and corrupt practices are common in their country, little changed from the last four years' surveys. Moreover, 32 percent say they have had personal concerns about bribery and corruption in their workplace.

The survey also reveals that whistleblowers remain a critical source of information on alleged misconduct—55 percent report that their company has a whistleblower hotline in place. Yet because of certain barriers, respondents indicate such mechanisms may not always be effective: 18 percent say loyalty to colleagues would deter them from reporting fraud, and 19 percent cite loyalty to their company as a deterrent. **—D. SALIERNO**

CLOUD AT THE TIPPING POINT

Security worries a barrier to trust in cloud services.

Business use of cloud computing services is becoming commonplace, with respondents to a recent Intel Security survey saying their organizations will dedicate 80 percent of their IT budgets to cloud services within the next 16 months. Yet, just as investments in cloud services are reaching a tipping point, many organizations don't trust them fully. The Blue Skies Ahead? report is based on interviews with 1,200 IT decision-makers in Australia, Brazil, Canada, France, Germany, Spain, the U.K., and the U.S.

Among those respondents, 77 percent say their organization trusts cloud computing more than it did a year ago, but only 13 percent say their organization fully trusts public cloud providers to secure sensitive data. Most enterprise cloud deployments (51 percent) use a private cloud model.

As more organizations invest in the cloud, building trust "will become integral to realizing the benefits that cloud computing can truly offer," explains Raj Samani, EMEA chief technology officer with Intel Security.

Building trust should involve educating business and technology executives on security risks. For example, although respondents say the C-suite is more involved in cloud decisions, only 34 percent say senior executives totally understand the risks involved. **—T. MCCOLLUM**

IMAGES: TOP, LEOLINTANG / SHUTTERSTOCK.COM
RIGHT, DOOMU / SHUTTERSTOCK.COM

Back to Basics

BY MICHAEL J. MARCUCCI EDITED BY JAMES ROTH + LAURA SOILEAU

THE FIRE DRILL

Auditors can learn to deliver a focused message that results in management action.

On the second day of an off-site meeting in New York City for GE Capital's audit leadership, the building's fire alarm began to blare while a voice announced "This is a fire drill!" over a loud speaker. Adhering to protocol, attendees filed out of the conference room into the foyer. As we waited for the usual speech about fire safety, people started staring down at their phones. Then Bill, the fire marshall, walked in and began to speak.

His conviction, intensity, and depth of expertise had a transformative impact on the leadership team. In the next 10 minutes, we learned more about fire safety than we ever have. We also observed a level of focus and clarity of thought that can be applied to our jobs as auditors. In five key areas, Bill's memorable performance reminds us that planning, competence, sales skills, focusing on the big picture, and being a catalyst for action are the hallmarks of a successful auditor.

Plan Your Work/Work Your Plan The fire drill started several days or even weeks before somebody pulled the red lever. Someone had to consider notifying building management, coordinating with local fire and police authorities, checking the equipment, allocating staff to manage the flow of people, alerting the security guards, and setting observation points to collect data for post-event assessment. Bill did the talking, but it was clear that there were a large number of people working as a team to ensure a smooth exercise.

Especially for managers, the complexity of the functions we audit, combined with the heightened expectations of our work, make effective planning critical. In fact, planning is the one area where managers can best influence the results. Very similar to an audit, the success of the actual event is highly dependent on the investment in planning. In GE Capital's audit methodology training, audit managers are encouraged to invest up to 40 percent of their time in the planning phase of the audit. That is because this is the point where experience from prior audits can be leveraged to guide the audit team. This means looking forward and using that experience to guide the team with a well-crafted plan.

Compensate With Competence Once Bill pulled us together—and quieted us down—he said he knew we were busy and would only take 10 minutes of our time. He marched through his punch list in an orderly manner and finished on time. Bill came prepared to do business, knew his material, and made the best use of our time. The content was dry and he knew our attention spans would

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

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

be limited, so he compensated with competence. Bill was articulate, informed, and concise. He had a well-rehearsed speech and got our attention with precise data points that were based on his experience and observations.

During an audit, getting the time and full attention of management can be difficult. When we are presenting findings to our stakeholders, we know they would rather be anywhere else, so we have to be in full sales mode. We sell assurance, and we do that by being informed, independent, and competent, and by backing up our observations with data and experience. This is core to the value that auditors bring to the organization.

Sell With the Passion of a Champion Not once during Bill's presentation did he mention policy or regulators. He never referred to third parties or higher powers to justify why he was there, nor did he apologize for what he was doing. He stated the key risks, articulated why we should all work together, and gave us valuable information. He did it with such passion and energy that in a few short minutes, a team of audit executives had become fire safety disciples. In this sense, he transformed his role into that of a sales person. He was selling safety, and we bought his pitch. In short, he was not a victim of policy, but a champion of safety.

When pressed by management as to why time and resources should be devoted to fixing a control problem found in an audit, the easy way out is to cite policy or regulators. But these alone are not sufficiently valid justifications for spending company resources and are a weak crutch for auditors to use. In fact, the best justification for spending company resources is fixing a control weakness that is causing an unacceptable risk. While we like to think that the title of "auditor" suffices in carrying the day, we ought to be more like Bill and sell our views to management with passion and expertise. Often we are asked for an opinion, which is part of the job, but that opinion is only as good as the analysis and facts that support it. Otherwise, it is speculation.

Internal audit's opinion is only as good as the analysis and facts that support it.

Communicate Big Risks Well Bill focused on the big picture. Fire safety for a building in Manhattan means being prepared, having a plan, and getting out safely. But there is more to it than that, such as descending stairwells, avoiding elevators, grabbing personal belongings, staying calm, knowing the exits, and securing your desk. By keeping us focused on the big picture, Bill kept our attention and left us with information that we would remember. In fact, he did such a good job that months later I still remember the basic ideas that he covered—be prepared, have a plan, look around, and don't panic while leaving.

Audits can be tedious and fieldwork can include weeks or months of tracing, reconciliations, interviewing, and other testing. This work forms the basis of our views, but the drama and grit of this effort does not need to be recited when delivering our final report and opinion to management. To add value, we need to convert the reams of data we obtained during the audit into useful information and frame that information in the form of key risks to the organization. Any competent executive will take immediate notice when you say words like, "the lack of controls around this process represent an unacceptable risk to the organization," but will immediately go to their smartphone if those words are "we spent three weeks reconciling 42 subledger accounts."

So What? This is a succinct way of asking, "Why are you telling me this and what do you want me to do?" Bill was very focused on the "so what." He taught us why a fire drill was important and how to prepare for the real thing. How often in an audit, a presentation to management, or any other meeting do we end up with an understanding of facts and risks but no action plan? After you hear the "so what" question enough times, you learn to start presentations by addressing this question up front rather than forcing people to wait for the inevitable. By addressing the lead point in the beginning, and by practicing your lines in advance to deliver a sharp and focused message, you can get management to act immediately on important control weaknesses.

This Is Not a Drill

As internal auditors, we perform a mountain of work under tight timelines with little visibility, only to have our efforts reduced to a sound bite or a few sentences in a presentation. But as Bill demonstrated, in those few moments that we have our stakeholders' attention, it is our job to deliver a focused message that results in management action. In the end, auditors add no value if we are not a catalyst for change in the organization. Ia

MICHAEL J. MARCUCCI, CIA, CRC, *is director of global audit operations at GE Capital Audit in Norwalk, Conn.*

BY HANS-ULRICH WESTHAUSEN EDITED BY STEVE MAR

THE TECH-SAVVY AUDITOR

Effective use of audit technology can enable audit departments to provide valuable insights.

According to The IIA's 2015 Global Internal Audit Common Body of Knowledge (CBOK) Practitioner Study, 62 percent of CAEs report their departments use technology infrequently and rely primarily on manual systems. While electronic workpapers have a high usage rate, about half of all internal audit departments say they use data mining or analysis software only minimally or not at all.

Internal auditors also have weak IT backgrounds. Thirteen percent of CBOK respondents have completed higher education in information systems or computer science, just 10 percent hold ISACA's Certified Information Systems Auditor (CISA) designation, and only 3 percent have an IT security certification.

That situation is not acceptable, because deploying technology and possessing IT knowledge are necessary components for internal audit to add value. A technology-oriented internal audit can provide internal support to software projects, identify weaknesses in data processing, and transfer data analytics know-how to operational functions. Adopting technology also can make audits more efficient.

The Case for Technology

The *International Standards for the Professional Practice of Internal Auditing* (*Standards*) requires internal auditors to be knowledgeable about IT risks and controls, as well as audit technologies. But sometimes internal audit's inability to leverage technology is the result of a poor audit environment, rather than a poor department.

Take for example a small audit department that has not audited double payments to suppliers; variable data such as transaction and accounting data sets; or master data contained in product, price, and customer databases. After the department's five auditors return to the office from a seminar about the use of big data analysis, the CAE proposes investing in a software tool. However, the company's chief financial officer rejects the proposal, saying, "We have a functioning enterprise resource planning system that automatically identifies potential double bookings. Therefore, double bookings and double payments are impossible." Knowing that double payments are always possible—costing the company an average of US$2,000 per case—the CAE plans a manual audit of suppliers' invoices instead.

CAEs can cite three reasons to justify greater use of audit technology. First, technologies such as data analysis and continuous auditing are more efficient and effective than manual audits, resulting in faster audits, cost savings, satisfied clients, and measurable value.

Second, proactive use of data monitoring and analysis software can significantly cut

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

TO COMMENT on this article, EMAIL the author at hans-ulrich.westhausen@theiia.org

fraud losses. According to the Association of Certified Fraud Examiners' 2016 Report to the Nations, such software reduces median losses from reported fraud cases by 54 percent (from US$200,000 down to US$92,000) and cuts the duration of such cases in half (12 months compared to 24 months) compared to organizations without that software in place.

Third, new business risks such as big data, cyber threats, and digital services demand a higher level of audit technology in the next few years. Although a 2015 PricewaterhouseCoopers study predicted that audit technology such as data analytics would be one of four priority capabilities for the profession, its 2016 State of the Internal Audit Profession Study reveals that just 40 percent of internal audit functions use technology.

Using Technology Better

The biggest technology challenge internal audit faces is finding a way to improve its ability to use audit software. CAEs and IT audit managers can take several steps to achieve that objective.

Demonstrate the Potential A broad base of theoretical and empirical data, experts' opinions, and *Standards* requirements support the need and usefulness of technology-based auditing. It might be motivating for "technology-oriented auditors" to provide testimonials about their experiences in using audit software. For example, an expert could give a live presentation of advanced tips and tricks for using Excel, which many auditors may not have tried before.

Training and Practice Internal auditors need adequate training to use the software. Training can include frequent practical IT challenges that must be fulfilled under supervision—such as extraction, set up, and analysis of files from databases—or joint audits in teams with experienced auditors. But training alone is not enough if the software is not used frequently to gain experience with it. Additionally, achieving certifications such as the Certified Internal Auditor or CISA can educate auditors about structured approaches for problem-solving such as IT models, standards, and best practices.

Build Know-how Depending on the organization's size, the internal audit department should consider establishing a data analytics center in-house. The center can enable auditors to

share experiences with audit technology through workshops and practitioner seminars. Smaller organizations should at least have regular meetings with external experts to gain such knowledge. In addition, rotating business and operational auditors to perform technology audits can help them learn best practices in using audit software.

Review Software Usage The process of investing in audit technology should not only follow a management decision, but also a review step. Some audit departments seldom use the software they purchase. Regular reviews of how the department uses audit technology can identify weaknesses and improve audit efficiency, such as reducing the time it takes to prepare data sets for analysis. Performing a software inventory check can locate and enable internal audit to leverage software the organization already has in place.

Management Feedback If management is dissatisfied with the current use of audit technology, but is confident about the value that digital technologies can create for the organization, internal audit should discuss how it is using audit technology with management. Internal audit can demonstrate the monetary value of audit results created with audit technology. For example, recovering US$10,000 from three double payments identified using analysis software can easily exceed the amount the department spent on a software licence.

An Effective Approach

Internal auditors do not simply need more audit technology, but also a more effective approach to using those tools to deliver value. Internal audit can start by reviewing how—or whether—it uses the audit software currently in place. Next, it should create a plan for integrating audit technology more into daily audit work. Measures can encompass training, adjusting audit plans with a stronger focus on IT aspects, and identifying potential technology gaps, such as equipment or training. Finally, the department should monitor its use of technology to ensure performance improvement. Ia

HANS-ULRICH WESTHAUSEN, PHD, CIA, CISA, CFE, *is head of Internal Auditing, ANWR GROUP eG, Duesseldorf, Germany.*

BY LARRY L. BAKER EDITED BY PAUL SOBEL

INTEGRATING KEY RISK AND PERFORMANCE INDICATORS

Internal audit can leverage its risk knowledge to improve operational performance and reduce risk exposure.

As risk management evolves and matures, many organizations are focusing more on performance management, which measures how effectively they are achieving their key business objectives. With this growing emphasis on performance, internal auditors should provide assurance and consulting advice regarding the achievement of objectives communicated to stakeholders.

An organization's strategic planning function and other functions provide management timely, useful information necessary for effective decision-making. However, many organizations have limited alignment among the groups providing information to management and the board. Also, one fundamental difference between these functions and internal audit is the use of a "performance lens" versus a "risk lens."

One way internal auditors can help create more alignment among functions is to encourage formalization and integration of top-down key performance indicators (KPIs) and key risk indicators (KRIs). KPIs are metrics that provide visibility into the performance of the business and enable decision-makers to take action. KRIs can provide an early signal of increasing risk exposure. Both types of indicators can give management and the board significant insight into how effectively the organization manages risks and resolves performance issues.

Implementing KPIs

Although KPIs and KRIs can add business and shareholder value, few organizations have implemented a sustainable process at the entity level that truly drives performance. Even fewer have integrated KPIs and KRIs into one seamless process.

To build executive support, it may be easier to begin by implementing KPIs. Internal audit can help facilitate the development of a sustainable top-down KPI management process, which must be aligned with corporate planning, goal-setting, budgeting and forecasting, and capital allocation activities. A project to develop an effective KPI management process will typically include several elements.

Project Charter A formal project charter, with executive sponsorship, helps ensure management support and alignment of activities as the KPI management process is developed. The charter clearly defines the business case, problem statement, project objective, project scope, resources needed, and project timeline. The problem statement and project objective are key to aligning KPI activities. An example of a problem statement is, "Our company does not consistently focus on the activities and metrics that

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

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

truly drive shareholder value." A project objective example is, "Implement an ongoing KPI management process that directs focus on the true value drivers of the business and total shareholder return."

KPI Framework The framework provides a high-level overview of the components necessary to ensure a sustainable process. Five major components include:

- A KPI management process with four major phases: KPI planning, performance measurement, reporting and action planning, and taking action and monitoring.
- KPI governance, with executive committee oversight, a steering committee, and a data governance council.
- KPI integration, with strategic planning, goal-setting, capital allocation, budget and forecast, and compensation.
- A KPI infrastructure, including organizational structure, operations leadership role, KPI vision and objectives, and technology support.
- A KPI culture/foundation, with common terminology, change management, communication, training, and continuous improvement.

Key Metrics Identification This element focuses on determining the few metrics that are most critical to driving business value and shareholder return. Whether the focus is on performance or risk, many times the word "key" is lost when deciding the appropriate number of metrics to measure and monitor at the entity level. Identifying about a half-dozen metrics can be a good start. This requires executive management to consider which metrics truly make a difference to the organization's success. For example, KPIs for an energy company may include production growth, operational expenses, and safety.

KPI Executive Dashboard Having a visualization tool in place enables management to easily review the organization's performance compared to targets and budgets. An effective KPI executive dashboard should graphically present a manageable number of KPIs that focus management's attention on the true value drivers of the business and shareholder return. The dashboard must be visually clean and easy to navigate. Using a simple color scheme—such as red, yellow, and green—can highlight performance levels in comparison with tolerances set by management. Features may include:

- A menu tab, including a drop-down list of specific KPIs and action plans.
- An information icon for each KPI, including the KPI definition, metric calculation, related goal, and data source.
- A KPI title, for metric clarity and ability to quickly view more detailed information about the KPI.
- Clearly defined and approved performance tolerances.
- A KPI current status indicator, highlighting actual performance versus target and budget.
- Hover-overs to highlight a further breakdown of performance for all business units.

Integrating Risk With Performance

Once a KPI management process is in place, organizations can follow a similar process to develop and integrate KRIs. Because internal audit has experience with identifying emerging and changing risks, auditors can help management determine the KRIs of most significance to business value and shareholder return. For example, KRIs for an energy company could include global macro-economics, commodity price volatility, stakeholder activism, and safety. These KRIs can be added to the executive dashboard to allow easy access to both KPI and KRI information.

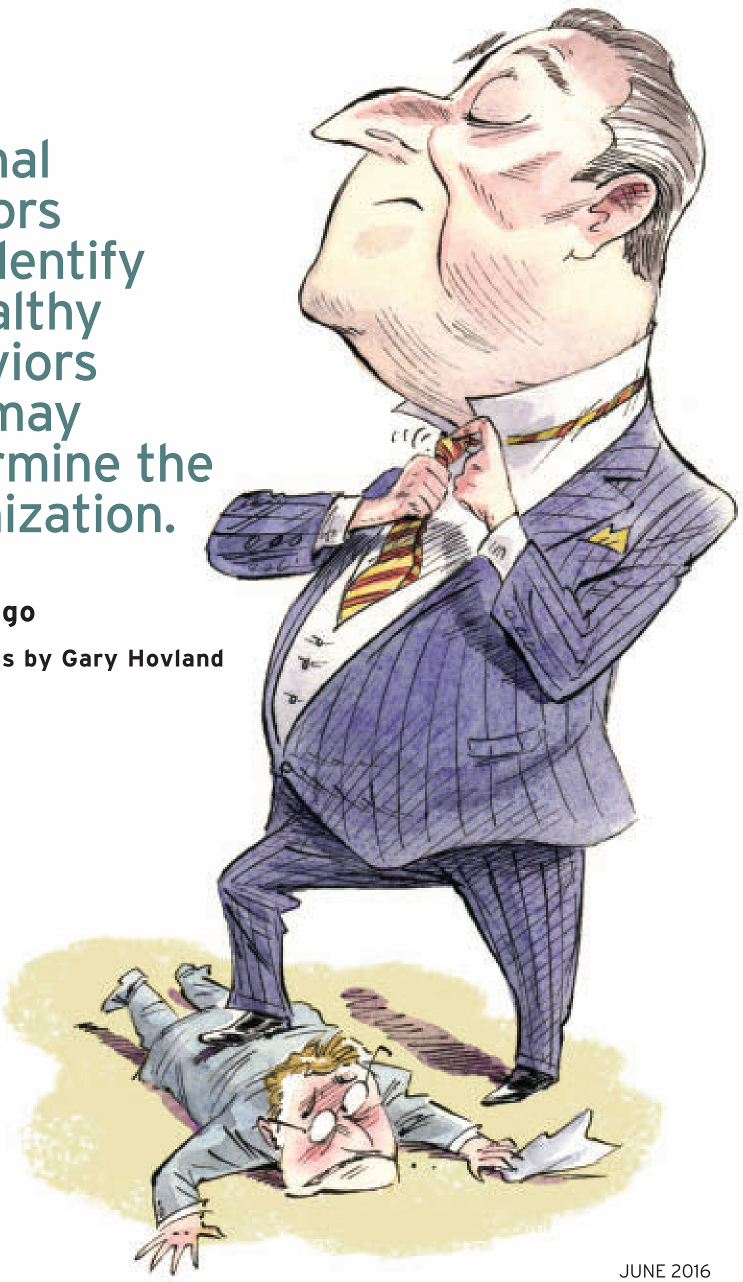
Depending on the level of transparency accepted by the organization's executive team, KPIs and KRIs can be monitored in the executive dashboard by management, auditors, and other leaders across the organization. For example, a safety-related KRI could track the number of incidents caused by mechanical failure. As the number of incidents increase, so does the likelihood of a serious injury or fatality.

Supporting Decision-making

To generate value, organizations must achieve or exceed performance goals communicated to stakeholders. To retain value, they must understand, monitor, and proactively manage significant risks to the achievement of key objectives. By facilitating the integration of KRIs with KPIs, internal auditors can help management gain timely, useful risk and performance information that allows it to make effective decisions. Ia

LARRY L. BAKER, CRMA, CCSA, CPA, *is a senior leader in internal audit, ERM, and strategic planning in Edmond, Okla.*

Toxic LEADERS



Internal auditors can identify unhealthy behaviors that may undermine the organization.

Jane Seago

Illustrations by Gary Hovland

Toxic CULTURE

Leaders whose negative practices sustain an unhealthy, even toxic, culture in their organization foment distrust, behave unethically, disempower employees, play favorites, and put their own needs and objectives first. In the words of Thomas O'Connor, director of internal audit at Urban Outfitters Inc., in Philadelphia, "Toxic leadership styles typically reveal a risky degree of incompetence at the management level."

Why spend time talking about such negative influences? Because culture affects organizational success. In a recent Duke University study, Corporate Culture: Evidence From the Field, 91 percent of North American CEOs and chief financial officers say culture is important to an organization; 91 percent say improving their company's culture will boost its value; and more than half say culture has a significant effect on productivity, company value, creativity, profitability, and rate of growth. Thus, knowing more about how a toxic leader can negatively affect an organization makes sense from a purely business point of view. Even more pertinent, internal auditors can take a prominent role in identifying these individuals and suggesting effective mitigation tactics.

SPOTTING THE BAD LEADER IN THE WILD

Recently a roundtable of internal audit experts at The IIA identified leadership traits that strongly correlated with an unhealthy organizational culture (see examples on the following pages). Upon reviewing these traits, Phillippa Foster Back, director at the Institute of Business Ethics (IBE) in London, summed them up neatly: "Power and control. They're all about power and control."

Take, for example, secretive leaders. They keep information to themselves because of the power it represents. Bethmara Kessler, CAE of Campbell Soup Co., in Camden, N.J., notes that they "perceive information as currency in the workplace. They want to be the ones who use it to advance in the organization." She cites the example of former Enron CEO Jeff Skilling using the term "black box" to describe the energy company's special brand of fraud. His joking about it, using a slightly absurd term, shuts down questions and ensures that the power of the information is contained to only a select few.

Robert Taft, CAE, University Audit, at the University of Central Florida in Orlando, points out that autocratic leaders also tend to be driven by power. They

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

THE AUTOCRAT
Egocentric and narcissistic, this leader possesses a strong feeling of entitlement. Autocrats are focused on themselves, not the organization, and will step on anyone who impedes their path to the top.

are often high producers—the organization's superstars. As a result, they may end up as the "face" of the organization or of a key function within the organization. That is not necessarily a negative, except when they use the exposure for their own benefit, rather than the organization's. These individuals can be more focused on their own greatness than the organization's success, may not be overly concerned about the organization's future performance, and may internally hope the organization struggles after their departure.

Of course, having a superstar is often of great benefit to the enterprise—think Steve Jobs—so they are not necessarily bad leaders. They cross the line, though, when they begin to believe they are above the rules and not to be questioned. Having a single dominant individual who does not encourage discussion, testing, and debate deprives the organization of the healthy give-and-take that tends to support collaboration, drive innovation, uncover problems in advance, and build competitive advantage. Ron Johnson, the former CEO of JC Penney, is an example of this type of autocratic leader, Taft says. A November 2015 *Fast Company* profile details how Johnson totally overhauled the JC Penney retail model without listening to anyone, ultimately alienating employees and customers—a scenario that ended with his termination.

Intimidators take such self-centered behavior even further by exercising power through fear. They seldom compliment or reward success. Instead, they accentuate the errors others make, thereby undermining morale, discouraging the sort of experimentation that often leads to breakthroughs, and potentially running off promising talent. "Fear and intimidation have been proven as effective management tools when there is underlying substance to produce positive results," O'Connor says. "However, a toxic management style typically masks the lack of that substance, causing the organization to lose valuable time going down a path that leads to poor results."

Manipulators, too, seek to maintain the illusion of power by using the latest buzzwords; cozying up to executive management, the board, and the media; staging flashy diversions from less-than-successful endeavors; and constantly seeking the next big thing while ignoring their primary responsibilities. Taft likens them to "one-hit wonders." Diana Henriques, financial writer and author of *The Wizard of Lies: Bernie Madoff and the Death of Trust*, calls the description of "the manipulator" on page 31 "a perfect recipe for the next Bernie Madoff."

Some toxic leaders are more driven by control. Closed-minded leaders do not like to be challenged. Tom Luccock, retired director of internal audit and senior adviser to the president at Michigan State University, indicates that those he has encountered "would often not explain what they wanted, but expected others to complete a task without direction." Deflectors seek to control their own reputation by sidestepping accountability for a failure or responsibility for fixing it.

Inappropriately focused leaders try to achieve and retain control by orchestrating results they consider important, to the detriment of the priorities of others. However, Kessler points out that this approach may be intended or unintended. For example, when an organization is struggling, an ethical leader may try to motivate employees by encouraging them to "do what it takes" to make that quarter's figures. The leader does not intend for employees to override company policy to make that happen, but an employee may interpret it that way. The leader's focus is not inappropriate; the employee's is.

AUDITING FOR BAD LEADERSHIP

Internal auditors must leverage their experience to flush out the toxic leadership styles that tend to do damage when they go unchecked. Like many aspects of auditing organizational culture, some techniques to accomplish this are subjective and some are objective.

55% of survey respondents say **behavior** modeled by top **executives** is the most effective factor influencing culture, according to The IIA's 2016 North American Pulse of Internal Audit report.

Subjective Methods Foster Back suggests starting with the traits of ethical leadership identified by the IBE: honesty, fair-mindedness, openness, courage, and ability to listen. Internal auditors can evaluate the degree to which these traits are present and how these individuals are perceived by peers and subordinates. She notes that some internal audit departments are bringing in employees with nontraditional backgrounds, such as behavioral psychology, to provide expertise in subjective analysis.

Psychology also can be useful in tailoring communication to the audience. For example, the internal auditor might comply with the leader's expectations as a way to open the door to delivering the necessary message. So, for the autocrat, this might entail saying, "Of course you are special, but here's what happens to the organization if you don't follow the rules." Luccock suggests a similar method of feeding the leader's ego by using questions that indirectly compliment him on how he was able to accomplish so much, thus giving him a chance to boast. This approach helped Luccock investigate a kickback incident at an earlier job in an energy company. After the individual admitted that he accepted kickbacks, Luccock inquired how he managed to do it—and received an explanation "in full detail!"

Henriques suggests questions that go straight to the heart of the individual's flaws. "One attribute of con men I have known is that they have an almost pathological need to always be seen as successful and an ingrained resistance to admitting failure in any circumstances." Keeping up a facade of consistent success requires them to skirt the truth on a regular basis. It is not easy to unmask good liars, but internal auditors may uncover some valuable indicators of dishonesty and cover-up by asking about past failures and listening carefully and skeptically to the answers. An inability to provide specific details about past projects, a hesitancy to describe exact processes and approaches taken, a reluctance to identify collaborators, and a refusal to share credit with others may be warning signs that the individual's successful track record is not all it appears.

THE CLOSED-MINDED
"My way or the highway" is their favorite saying. Close-minded leaders thrive on a high-control, low-inclusion environment and favor working with yes-men, who conform to their intolerance of dissent.

THE MANIPULATOR
These leaders function mainly on the surface, not surprising given their extreme image-consciousness. Often quite charming, they can easily deceive others.

Kessler points out, though, that internal auditors should never confront a toxic leader. It is important to recognize that an audit is not an investigation. She elaborates, "If, in the normal scope of an audit, the auditor uncovers evidence that would tend to indicate there is a toxic leader in the organization who is undermining controls, it is time to step outside audit mode." The auditor should speak with the company's legal counsel or its compliance officer, explain the reason that an investigation may be in order, then, Kessler emphasizes, "follow the company's established investigative protocols."

Objective Methods Some tried-and-true objective approaches can be quite

effective. For example, these toxic leadership types tend to cause employees to flee the company. Therefore, it is worth looking at turnover rates and exit interviews, which will reveal the number of employees who have left and the reasons why. Employee engagement surveys may provide advance notice of problems by revealing the leaders that employees are grumbling about and why.

Reviewing the individual's consistency in submitting required paperwork also can be enlightening. As Henriques points out, those with a "rules don't apply to me" outlook often manifest "a refusal to adhere to sensible documentation requirements established for budgets, expense accounts, invoicing, cybersecurity, etc."

Other potential evidence to reveal toxic leaders includes a history of litigation and regulatory issues, and a tendency to employ relatives, especially if they are not qualified for the positions they hold. Because many of these leaders don't take responsibility for failures or mistakes, or simply do not have the commitment to complete a project, there may be value in seeking evidence of their involvement throughout a project. Excessive travel or use of organizational resources for personal use might also be a red flag. Taft notes that bad leaders may believe "they deserve it."

THE SECRETIVE
This leader avoids transparency, failing to share information before a decision is made or the results of the decision afterward. Secretive leaders play favorites with employees and are unusually connected with outside parties such as customers and consultants, of whom they are quite protective.

BEYOND THE QUESTIONS

The work internal auditors do in gathering evidence is necessary and valuable, but the real benefit to the organization comes after that, in the work internal auditors do to help prevent the recurrence of counterproductive behaviors or contain their damage. Luccock suggests, "Offering timely and constructive suggestions and clear paths forward often helps direct some negative types of leaders to improve controls."

Toxic leaders may exercise control because they believe they are operating in out-of-control conditions. Therefore, they may favorably receive substantive guidance on how to create order out of chaos. Until that results in a change in the leader's behavior, however, Luccock advises counteracting an inappropriate concentration of control by recommending a separation of duties to ensure adequate checks and balances.

THE DEFLECTOR
These leaders tend to avoid responsibility if a project fails. Their first reaction is denial; they go into "attack mode" if challenged. The Deflector does not seek the root cause of problems, but instead prefers talk over action.

In the same vein of providing constructive suggestions to change behavior, inappropriately focused leaders may respond well to a demonstration of the benefits to the organization of rebalancing their priorities. "Use experience and facts as much as you can," O'Connor suggests. "Since they may not understand the problem, coach them through a solution."

These recommendations may be appropriate within the scope of a normal audit—perhaps when the leader's behavior is disruptive, but does not bypass controls—provided the internal auditor has discussed the

VISIT our MOBILE APP + InternalAuditor.org to watch IIA President and CEO Richard Chambers discuss the importance of organizational culture.

THE INTIMIDATOR
As the name suggests, this leader fosters an atmosphere of fear and intimidation, overreacting to others' mistakes and punishing failure rather than learning from it. Intimidators have a "kill the messenger" attitude and lack empathy for others.

recommendations with the CAE to ensure they are constructive, not confrontational. However, sometimes a leader's behavior goes beyond certain boundaries and is so egregious it must be reported through appropriate channels. If the leader is at a senior level, the CAE should report the concerns to the board or the audit committee. If the leader is a middle manager, then a word to the senior vice president or vice president is advised. If the leader's actions are beyond poor behavior and instead constitute a known violation of policy, such as fraud, Taft recommends following approved investigation guidelines and creating detailed documentation to keep the focus on the issues as opposed to the emotions and personalities involved. It is advisable to involve the ethics, legal, and human resources functions in these instances.

LEARNING A LESSON

There are lessons to be learned from interaction with toxic leaders, unwelcome though that interaction may be. Engaging with challenging leaders is an opportunity for internal auditors to polish their skills in asking open-ended questions and listening to both what people say and how they say it.

It also is an opportunity to recognize that things are not always what they may initially seem to be. Most people exhibit some of these undesirable behaviors from time to time without belonging to one of the "unhealthy leader" categories. Internal auditors always have to investigate further and take a bigger-picture view. "Everyone has an occasional bad day," Kessler points out. "You have to look at their pattern of behavior, not just your short engagement with them."

THE IMPROPERLY FOCUSED
These leaders focus on inappropriate and unbalanced objectives, pursuing their own goals over company strategies. They are likely to emphasize the "what" over the "how." Their motto? The ends justify the means.

Ultimately, despite all best efforts to follow standards, establish quality controls, and apply good practices, some leaders will be toxic. Internal auditors must remain vigilant in spotting them and taking appropriate steps to help identify the situation so it can be addressed through established processes.

O'Connor often flashes back to his time as a loss-prevention officer at Tiffany & Co.'s in New York City, a busy store containing immensely valuable items. Each day, tourists would come into the store to marvel at the magnificent jewelry. "It was an amazing experience to stand and monitor the crowd: hundreds of people, all basically following the pattern of a shopper—except for the three or four people who are not, the toxic outliers," he recalls. "It's the same for managers in an organization. There are going to be those outliers. With our unique experience, internal auditors can help keep the honest people honest as well as identify the truly toxic leaders before they cause too much damage." Ia

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

Analytics & the small audit department

No matter the size of an audit function, analytics can be implemented for big gains.

Jared Soileau
Laura Soileau

Many small audit departments grapple with how to use analytics to audit more efficiently. The value added through analytics is regularly discussed in research, thought leadership, and industry publications. And most auditors would readily capitalize on an opportunity to do more with less. The challenge for those audit departments with constrained resources is not what to do, but rather how to go about doing it.

Small audit shops can leverage analytics and use tools already in place to implement analytics within their audit functions, reducing the need for a potentially costly up-front investment. Many of the metrics historically used to measure business performance are analytics. Examples include variance analysis, benchmarking, return on assets, turnover (inventory, accounts receivable, employee), reorder points, credit limits, and even Benford's Law. With this in mind, small audit functions that think analytics may not be within their grasp should reconsider.

With the right approach, moving analytics from concept to practice can be simple.

GETTING STARTED

Analytics can be used at various phases of the internal audit process, including the risk assessment process, macro-level audit planning, and micro-level audit planning. During risk assessment, analytical data can be used in combination with qualitative data to better understand and prioritize the organization's risks. At the most basic level, analyzing financial and operational information, prior audit findings, and key performance indicators (KPIs) across the enterprise can be a useful tool in completing the risk assessment. At macro- and micro-audit level planning, analytical data can be used to assess specific controls and to examine existing and emerging risks. This will help determine specific areas of audit coverage and the extent of testing within each area. The size of the audit department should not be the only factor in determining whether to implement an analytics program, as there are analytic tools that can be used even by one-person audit departments.

With the right approach, moving analytics from concept to practice can be simple. As an internal audit department of any size begins using analytics in its audit process, an important first step is determining what it wants to understand. The analytics initiative must have clearly defined goals and performance measures. Further, internal auditors should critically assess the questions they need to ask to ensure they understand how the business objectives and operating cycle will impact the underlying data to be analyzed.

Organizations may have different responses to the same question. For example, "How does weather influence your organization?" will have different meanings and different outcomes, depending on the industry. Thunderstorms may drive ticket sales for movie theaters while they wreak havoc on energy providers. In addition, the time of year, day of week, time of day, and geographical location likely will impact how weather influences any organization. In this situation, there is no right or wrong answer—it's what makes sense for the organization.

There are numerous questions an internal auditor may want to answer with the analytics program, which should closely correlate with the specific objectives of the program, itself. Examples include, "How frequently are credit limits overridden?" as related to the order-to-cash cycle; "Is inventory turnover in line with historical and/or budgeted averages" related to the inventory cycle; and "Do company buyers have an over-reliance on key vendors?" related to the vendor management process.

POTENTIAL ROADBLOCKS

Internal audit departments often fail to identify the correct data source for the data to be analyzed when beginning an analytics program. Selecting the wrong source could be detrimental to getting an analytics program up and running; therefore, a critical decision is determining which data sources are the most appropriate to address the questions being asked. Several ways to overcome such roadblocks are to review the preliminary data, determine whether there is anything in the data that raises questions, and ask questions to confirm and validate the accuracy of the data source.

Similar to validating the criteria used to assess the audit entity, auditors should validate that the data can be used to address audit objectives. To do this, understanding the business, including typical operating cycle and key drivers that influence relationships within the data, is critical. The ability to look beyond the data to understand what it does or does not represent (e.g., identifying all systems in which revenue/expenditure transactions are recorded and confirming data files being used contain both accurate and complete data for the entity being analyzed) and application of critical thinking skills also are important steps in steering clear of roadblocks. Finally, this often is an iterative process, in which there may be multiple conversations with the data and business process owners before determining whether the data source contains the specific information needed to answer the questions at hand. Simply asking, "Can this data be used to answer the audit objective?" will smooth the path not only for obtaining the data but also accepting analysis results.

BRAINSTORMING

Although the fraud brainstorming process documented in the American

Data analysis tools – statistical analysis – ranks No. 1 in audit process knowledge areas that need improvement, per Protiviti's 2016 Internal Audit Capabilities and Needs Survey.

Institute of Certified Public Accountants' Statement on Auditing Standards No. 99 (SAS 99), Consideration of Fraud in a Financial Statement Audit, is not required for the internal audit process, research has demonstrated that it is an effective tool when used within the internal audit activity. While fraud is only one consideration of an analytics process, brainstorming should help identify key data and relations that should be evaluated.

One starting point is reviewing significant audit reports from the prior year. For example, in analyzing audit reports with low ratings, and considering uncontrolled risk or ineffective controls, the auditor could identify potential data points that would improve monitoring of the process in question. Likewise, in analyzing audit reports with high ratings, the auditor could identify potential elements in the process-level risk management that could be leveraged for other processes.

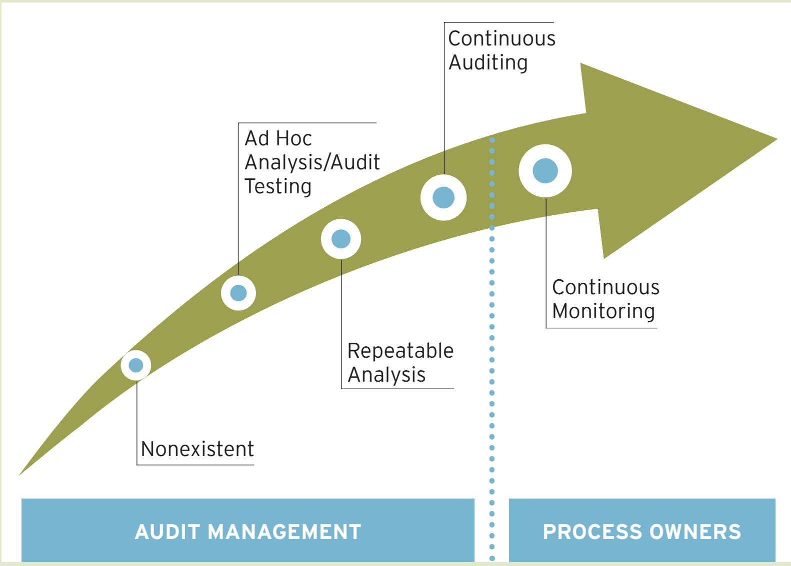
Another approach is asking management in risk assessment interviews, "What are the most important KPIs you are managing?" and follow-up questions such as, "What are the key variables that impact those specific KPIs?" Brainstorming during the internal audit planning process can identify additional factors that may impact those KPIs that are not already being considered.

Brainstorming also can be used in the evaluation of various company-generated reports to identify if there is information that may be further explored for additional insight. Financial statements and reports are great tools for understanding relationships in financial data and brainstorming where additional analysis may add value to the audit process. Other examples of using company-generated reports for brainstorming include evaluation of employee hiring and turnover reports as compared to historical and industry averages, review of inventory metric reports as compared to budget as well as prior year, and analysis of asset reports to consider whether the percentage of lost or stolen IT assets has increased or decreased.

ANALYTICS MATURITY CLASSIFICATION

There are several ways to progress an analytics program's maturity:

- Treat analytics as a "project" with appropriate management, goals, performance targets, and oversight.
- Establish clearly defined objectives for the analytics program.
- Involve business process owners, IT, and all auditors.
- Provide adequate resources, timing, expertise, training, and management support to the analytics function.
- Maximize the use of existing tools and reports.
- Track and report on analytics function performance.
- Build processes and procedures that address the challenges of today but also support future analytics capabilities.



ANALYTIC METHODS

Another important consideration for small audit departments is the analysis methods to be used. Some examples of analytic tools that can be used by small audit departments include correlation analysis, regression analysis, Benford's Law, and visualization. Internal audit functions may already be using several of these tools, but they may not be commonly thought of in terms of analytics. When identifying desired relationships, the analytic method should be considered when identifying data and sources necessary to perform the analysis. The analysis that the auditor is interested in performing, and the extent of data available, will dictate the analytic method to be used and the tool that can assist in facilitating analysis.

It is critical to have a plan that will allow internal audit to continue to improve its analytics capability.

Correlation analysis is the comparison of X and Y to see how they relate to each other. An internal auditor might use correlation analysis in a production process audit to measure the strength of the relationship between product defects and factory overtime. If the association is strong, the auditor might then use inquiry and observation to assess whether an overworked and stressed labor force is the cause of the defects, or perform regression analysis to predict future defects and then confirm the projection against actual defects that have occurred. This would allow the audit team to add some discussion of the coefficient of determination; namely, how much of the change in product defects is explained by the change in overtime.

Regression is the functional relationship between two or more correlated variables that is often empirically determined from data and is used especially to predict values of one variable when given the values of others. It can be used to evaluate the association between X and Y when a control exists for other known relationships. For example, in the event that overtime and employee turnover are both increasing, then regression analysis would provide for a more thorough analysis of what is causing the increase in defects. This would potentially allow for identification of changes, which may directly address the root causes and implementation of actions to bring the defect rate to an acceptable level.

Benford's Law is a theory based on a logarithm of probability of occurrence of digits (pattern anomaly of leading digits). Benford's analysis may allow small audit functions to more efficiently analyze revenue and expenditure transactions based on whether unexpected patterns exist within operations. Such analysis could be conducted across the entire organization, as well as within divisions or functions to identify additional risk concerns. This would be beneficial if there are specific data patterns associated with errors or potential fraud activities. One such example from M.J. Nigrini's *Forensic Analytics: Methods and Techniques for Forensic Accounting Investigations* would be an analysis of organizational expenditures. Although on the surface we may expect the first (two) digits of invoices would have an equal likelihood of occurrence, according to Benford's, the pattern of occurrence is not uniform, but a declining logarithmic pattern from 1 (10) to 9 (99). More specifically, the likelihood of "1" being the leading digit in a random number set would be 30.1 percent compared to 4.6 percent for the occurrence of "9" as the leading digit. Using Benford's analysis to evaluate invoices would identify specific leading digits of transactions, which should be further investigated via substantive testing. While initial analysis may not identify fraud, it identifies potential transaction anomalies, which may be linked to inappropriate expenditures.

Visualization comprises graphs and charts that often tell a story that is not easily understood by looking at the data alone. The internal auditor might use visualization to analyze the number of lost or stolen laptops year over year to evaluate whether laptop theft/loss is increasing or decreasing. Perhaps even further, the auditor could determine whether there are certain locations or business units that are driving the trend. If the trend line shows the number is increasing, the auditor might investigate to understand the root cause for the increase, including evaluating the effectiveness of the controls in operation.

SOFTWARE TOOLS

Tools to perform computer-assisted audit techniques have improved and expanded capabilities during the past two decades. While the internal audit profession has traditionally considered such tools as analytic tools, there are many additional tools that can be used in analytics. However, during the initial phases of developing an analytics program, particularly for small audit departments that may have more limited budgets, it may be more valuable to use tools that are already in place within the organization.

One objective in the early phase of analytics is attaining small wins to make the case for expanding the use of analytics. In many cases, small wins

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

can be more easily achieved when the investment cost is low. Given that Microsoft Excel remains one of the top analytical tools used by internal auditors, its versatility and ability to perform each of the previous analytic methods allows it to be a first step in implementing an analytics program. However, despite all of its flexibility, data limitations (Excel is limited to 1,048,576 records of data) may prevent the use of Excel during early stages of program implementation.

While starting small can produce early successes, it is critical to have an analytics plan that will allow internal audit to continue to improve its analytics capability. This should include a path that is scalable so the early successes can be built upon and not thrown away.

As the use of analytics matures and evolves, many organizations ultimately reach the continuous monitoring phase, in which process owners are responsible for continuous analysis of key risk areas (see "Analytics Maturity Classification" on page 37). Furthermore, team members will be much more likely to understand the broader software needs to expand the analytics processes. With greater understanding of functional needs, software selection may become a greater consideration, given the cost of the software as compared to the expected benefit to be received.

IMPLEMENTATION TIPS

Despite rapid changes in technology, many audit functions have not significantly modified their audit process to keep up with the data available as a result. While change can be difficult, it often provides increased opportunity to maximize the value that internal auditors can contribute. Although this contribution may be a lengthy process, failing to implement analytics into the audit risk assessment, testing, and monitoring processes limits the value that can be provided. So whether it's for the next risk assessment or audit, consider when, where, why, and how to use data in the process. Starting small is better than not starting at all. Ia

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

BUSINESS at RISK

PHOTOGRAPH: ASERGIEIEV / ISTOCKPHOTO.COM

Keynote speakers for this year's IIA International Conference identify emerging risks facing organizations.

Russell A. Jackson

Ask experts in business risk what makes them most nervous and many will name some aspect of a cybercrime or cybersecurity issue. That's relatively new; only in recent years has the specter of lost or stolen data—or worse—risen to the top ranks of corporations' concerns. Others may cite less technological issues, such as the threat of reputational harm, or political and economic uncertainty. But regardless of which areas pose the greatest concern, or how long they've been on management's radar, experts agree that audit leaders with a clear vision and a competent team are a key asset in coming to grips with them.

When internal auditors from across the globe gather in New York City in July for The IIA's International Conference, they'll be facing head-on many of the risk-related challenges businesses encounter. The assembled audit professionals will hear about risks and responses from speakers from all over the world, including five distinguished keynoters with a broad range of collective experience and backgrounds. *Internal Auditor* recently spoke with these individuals to gauge their views on emerging business risks, as well as the important role audit practitioners play in helping to address those areas.

DIGITAL DANGERS

Many businesses have elevated cyber risk to the top of their priority list. Indeed, says Julia Gillard—Australia's prime minister from 2010 to 2013 and, since, a lecturer, author, and fellow and board member of several institutes and organizations—hackers' growing sophistication, combined with the ever-increasing interdependence of cyber networks worldwide, represents perhaps the biggest near-term security risk companies face. "The best antidote, aside from constructive work with governments to appreciate and help manage cybercrime," she says, "is consumer education, so that individuals and businesses, including small businesses, can

VISIT OUR MOBILE APP + InternalAuditor.org to watch a video on internal audit's role in the expanding landscape of risk.

be more aware of what they can do to take prudent steps to protect their interests." Gillard adds that she has a deep appreciation from her experience as prime minister for internal auditors' role in that—especially by helping to ensure organizational integrity—and, generally, for how they work and the businesses with which they interact.

How big could the impact of cybercrime be on business? Richard Quest, CNN international business correspondent and host of the programs Quest Means Business and CNN Business Traveller, says simply: "Huge." By way of illustration, he adds: "In the past six months, I have received hack advisories from one of my credit card companies, my main bank, my health-care company, and at least two stores where I have shopped online." Large companies, he adds, may face as many as tens of thousands of hack attempts every day. He cites ransomware, which is becoming a real threat for hospitals, and notes that the Sony hack "showed us how damaging it can be when your confidential emails are dumped into the public domain."

IIA President and CEO Richard Chambers also fears the growing menace of cybercrime. "Beyond the volatility of an increasingly dynamic global economy, where new risks and disruptions can develop overnight," he says, "boards and managements have consistently identified cybersecurity and the ills associated with cyber breaches as the biggest business risks. This is likely to remain the biggest threat in the foreseeable future." Organizations are starting to realize that cybersecurity involves more than just efforts to stop attacks, he explains, and thus there's an increasing focus on how to identify and respond to cyber breaches when they inevitably occur. That response should include the same elements as any crisis management engagement: customer relations, brand reputation, and business continuity.

Large companies may face as many as tens of thousands of hack attempts every day.

Of course, that's easier to accomplish when the risks aren't morphing so rapidly; with cybercrime, the frequency and sophistication of attacks are both increasing constantly. "People are addressing it," notes Olivia Kirtley, president of the International Federation of Accountants and chair of the audit committees at Papa John's International, ResCare Inc., and U.S. Bancorp, "but you're addressing against a very active, increasingly capable environment, not a static environment. Trying to keep pace is one of the big risks out there."

POLITICS, THE ECONOMY, AND TERRORISM

Politics weighs heavily on Gillard's mind when it comes to business risks. "The collapse of so many nation states in the Middle East has not yet run its course, and the aftermath will continue to be troubling," she notes. As well, she points out that the entire world pays great attention to political developments in the U.S.; in her travels, the presidential election in particular comes up often. "To the extent the U.S. registers insecurity and turns inward," she says, "as opposed to expressing confidence and engagement with the world,

"The collapse of so many nation states in the Middle East has not yet run its course, and the aftermath will continue to be troubling."

Julia Gillard

"Auditors should use corporate culture to their advantage, aiming to show that they are part of the wider team that's ensuring the long-term success of the company."

Richard Quest

50% of executives say the risk management process in their company is not aligned with business goals, according to a 2016 survey by the Ponemon Institute and Shared Assessments Program.

this will have a big influence on perceptions of risk." Balancing that, she calls for "great confidence and optimism from the rise of Asia." The continent, she explains, is creating the largest middle class the world has ever seen, and Australia and the U.S. are well-positioned to serve it, with exports in technology, services, health care, education, tourism, and food.

In Europe, Gillard adds, other specific concerns include terrorist attacks and the upcoming vote in the U.K. on leaving the European Union. She also points to "overall, slower economic growth than we want and need" as a particular business risk.

The economy also concerns Paul Sobel, vice president and CAE at Georgia-Pacific LLC, as a business risk. His organization continues to feel the pinch of a housing market that "hasn't bounced back very quickly," which hurts Georgia-Pacific's building products business; it's already burdened with overcapacity, he adds, as new capacity has come online faster than demand has risen. Overall, he sees the world much the same way Gillard does. "Political, socioeconomic, and terrorist events cause unexpected changes in so many ways," he says. "Combined with rapid technology change and disruption, an organization must be continuously monitoring the external environment and updating its risk profile."

REPUTATIONAL WORRIES

For Kirtley, reputational risk also ranks high, especially with regard to social media. The problem, she notes, is that social media poses risks that aren't always within an organization's control. "For word to travel, it doesn't have to be true," she explains. "You're not just combatting things that might have gone wrong, you're combatting false information, too."

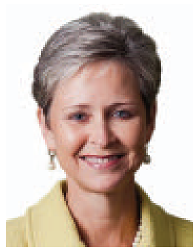
The best an internal audit shop can do is basically what it does in the face of any business risk: Make sure the organization has processes, procedures, and controls in place. "The veteran internal audit shops are shifting from being a participant in the risk-control environment to being an auditor of the risk-control environment," Kirtley says. "Are the risk mitigation plans in place? Are they robust? Are they functioning as they are purported to be?"

TAKING AIM

Indeed, internal audit's role in addressing many of the emerging business risks the experts fear most will be largely the same as for the risks companies already deal with all day every day. First and foremost, Sobel says, that means understanding how value is created and measured, so that the internal audit function can focus on its expanding mission of enhancing and protecting organizational value. "We must go beyond talking a downside risk language," he says, "to more of a value language that recognizes how we can enable future value creation, as well as preserve existing value."

That should help in accomplishing another one of internal audit's primary aims: being viewed as effective without destroying the trust in the department that's essential for its effectiveness. Establishing trust, in fact, is a "fundamental issue for internal auditors," Quest says. "Auditors should use corporate culture to their advantage, aiming to show that they are part of the wider team that's ensuring the long-term success of the company."

Doing that requires strong leadership, especially in the areas of communication, relationship building, and business acumen. "To reach the long-stated goal of becoming trusted advisers to management and the board, internal audit leaders must nurture skills that help meet growing stakeholder demands and offer valuable foresight to the organization," Chambers says. Successful



"The veteran internal audit shops are shifting from being a participant in the risk-control environment to being an auditor of the risk-control environment."

Olivia Kirtley

"To reach the long-stated goal of being trusted advisers ... internal audit leaders must nurture skills that help meet growing stakeholder demands and offer valuable foresight."

Richard Chambers

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

> An organization must be continuously monitoring the external environment and updating its risk profile."
>
> Paul Sobel

communication is a two-way street, he adds. Not only must internal audit leaders be able to successfully impart audit recommendations, knowledge, perspective, insight, and foresight, they also must clearly understand stakeholder needs and priorities.

Like many customer-facing operations, internal audit is a people business, and understanding stakeholders happens best when auditors actually know who they are. "Internal audit leaders must develop a rapport with management and the board that builds trust and credibility in the audit function," Chambers says. They must also understand the risks facing the specific industries they serve, he adds, and identify and monitor all associated key risk indicators. All the while, internal audit needs "a holistic understanding of the pressures and challenges facing management and the board," he says.

Gauging those risks and challenges can be difficult when stakeholders aren't working from the same page. "You often find when you survey about risk that there are different views on the risk appetite of a particular area or the overall risk environment and risk culture," Kirtley notes. "One of the more important things internal audit can do is to assure that there's a common understanding as to what the risk appetite and risk culture are. You've got to make sure everyone is in agreement." Indeed, she adds, it's imperative that internal audit pull that concordance down out of the theoretical and assure it's actually happening on the ground. There could be a disconnect in just two or three of, say, 10 areas of needed agreement, she

Economic slowdown in the U.S. and Europe ranked among the top five risks for 37% and 24% of respondents, respectively, in a 2016 survey by U.S.-based Depository Trust & Clearing Corp.

says, but they could well be the most critical two or three.

Sobel emphasizes that in all things, internal audit must be seen as a key facilitator and enabler of effective risk management. "It must be culturally acceptable, and even required, for internal audit to evaluate and provide advice and assurance related to the effectiveness of risk management," he asserts. Culture affects everything an organization does, he adds, emphasizing that the tone at the top and executive support must be clear in terms of the enterprise's risk criteria—such as risk-taking philosophy, risk appetite, and risk tolerance.

AGILITY AND SPEED

For all the emphasis on well-established practices being used in the face of emerging business risks, it's critical as well to see things in a different light and adopt previously unused tactics to move the organization's control environment forward. "In the immediate post-Enron world, the focus of internal audit was on providing assurance on financial reporting and compliance to a bevy of new reporting requirements," Chambers says. "Technology and cybersecurity issues have changed that." And those two issues, in one form or another, will likely continue to be the dominant forces on how business risks change. He agrees with Gillard and Sobel, though, that you can't discount economic volatility, geopolitical relations, and terrorism as factors that could dramatically alter business risks.

That's why Chambers urges internal audit practitioners to learn to "audit at the speed of risk." Internal auditors must become more nimble and agile in their ability to respond to increasingly volatile risk environments, he says, and that means expanding skills to meet those changing risks—and the related stakeholder needs, which are also changing. Internal audit departments should also emphasize constant investment in continuing education, developing business acumen to understand all the factors that influence the organization, and looking toward technology and innovation to improve how they do their work. As organizations' risks and other challenges continue to evolve, so too must the internal audit function. Ia

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

An Anti-corruption Checkup

Paul J. Morrison

Capability maturity models can help organizations assess the effectiveness of anti-corruption programs.

Revelations from the Panama Papers investigation paint a picture of public officials and business leaders allegedly moving money to secret offshore companies. The investigation by the International Consortium of Investigative Journalists is based on more than 11 million emails, documents, and client records leaked from Panama-based law firm Mossack Fonseca. Although much of the business operations highlighted in the papers are legal, some of the dealings allegedly include money laundering and other illegal activities, and the lack of transparency involved often is a red flag of potential corruption.

With the spotlight now shining brightly on potential corruption, it's more important than ever that organizations have comprehensive anti-corruption compliance programs in place. One way internal auditors can help management gauge the effectiveness and completeness of their organization's program is by using an anti-corruption maturity model. The maturity model depicted in this article is a variation of the capability maturity model integration approach developed at Carnegie Mellon University that has been customized to measure the proficiency of an anti-corruption compliance program. The model measures an organization's proficiency in complying with laws, such as the U.S. Foreign Corrupt Practices Act and the U.K. Bribery Act, by comparing its compliance program against anti-corruption standards.

Moreover, internal auditors can use the anti-corruption maturity model to measure the degree to which the organization has implemented governance controls and identify expectation gaps that may exist between the organization's perceived efforts and actual efforts. The model can enable auditors to identify areas of strengths and weaknesses, and it can serve as the basis for allocating resources to most effectively reduce corruption risk. In addition, auditors can use the model to measure the degree to which their organization has adopted regulatory guidelines in its anti-corruption efforts.

DESIGNING THE MATURITY MODEL

The anti-corruption maturity model measures control strengths on a scale (see "Maturity Model Scale" on this page). Each of the scale's four levels describes a different strategy for combating corruption. The model's scale should be commensurate with the organization's complexity, geographic dispersion, and capital resources. For simplicity, this model is designed for a mid-sized company that has multiple product lines and sells in a global market. A large company that has many subsidiaries operating across diverse industries might be better suited with a larger scale, perhaps with five or six levels. The size of the scale is not as important as having a scale that is aligned with the organization's risk profile.

MATURITY MODEL SCALE

ACTIVITY RANKING	COMPLIANCE APPROACH
LEVEL 4 Optimized	**Zero tolerance for corruption.** A compliance committee reports to the audit committee or board. Oversight is assigned to one or more senior executives who are accountable for implementation, have appropriate authority within the organization, have adequate autonomy from management, and have sufficient resources to ensure that the compliance program operates effectively. Risk assessments identify regions where rule of law is at risk, and controls are implemented before new regulations take effect.
LEVEL 3 Advanced	**Zero tolerance for corruption.** A strong board of directors and robust entitywide controls support zero tolerance. Risk assessments are conducted to assess changing conditions and identify areas that are highly susceptible to bribery. A well-staffed internal audit department regularly tests controls in all relevant risk areas to ensure they remain effective.
LEVEL 2 Reactive	**Low tolerance for corruption.** Controls are enhanced in areas where regulatory enforcement activities have been heightened. Process managers or supervisors are responsible for oversight and implementation of compliance controls. A small internal audit department tests corruption controls as part of other audits.
LEVEL 1 Basic	**Accepts elevated levels of risk.** Small, often start-up companies led by risk-taking entrepreneurs or private companies operating "under the radar" may be more risk tolerant. A feeble internal control structure is driven by the misconception that bribery is a legal, acceptable, and necessary cost of doing business in certain regions of the globe. Management views internal controls as a bureaucratic nuisance and assumes the risk.

Organizations in **101 countries** and governments in **11 nations** use capability maturity models to elevate operational performance and economic development, the CMMI Institute reports.

After an appropriate scale is established, internal auditors should establish the criteria on which the compliance program will be measured. Corruption-related controls should be grouped into components based on the risk drivers they are designed to mitigate. A Resource Guide to the U.S. Foreign Corrupt Practices Act, Hallmarks of Effective Compliance Programs, developed by the U.S. Department of Justice and the Securities and Exchange Commission, is an excellent resource for identifying the types of components that make up the foundation on which an effective compliance program should be built. This guidance identifies seven components that form the basis for the anti-corruption maturity model: oversight, resources, risk assessment, policy statements, due diligence, controls and monitoring, and training.

COMPONENTS

"Anti-corruption Maturity Model Components" on page 50 describes some controls that are typical of each component. Internal auditors should consider the organization's size, complexity, and risk profile in identifying which components to include in the model. For example, an organization that plans to grow through acquisition might add a separate component dedicated to the merger and acquisition process, while a company that does not rely heavily on third-party consultants or agents might place due diligence under risk assessment.

After identifying the controls relevant to the organization, the internal auditor should assign them to the respective component of the maturity model. Basic controls that by themselves are not effective in preventing or detecting corruption should be assigned to lower levels. As controls become more sophisticated and effective, they should be assigned to the appropriate higher levels. It is necessary to achieve the activities on the lower levels of the scale to attain those on the higher levels. Depending on the number of controls identified for each component, it may be more practical to summarize the objectives of the controls in the model, itself. The individual controls and their objectives will be detailed in the assessment test schedule.

As controls become more sophisticated and effective, they should be assigned to the higher levels of the model.

ASSESSING COMPLIANCE PROGRAM CONTROLS

Assessing an organizational-level compliance program goes beyond identifying risks and controls, and evaluating their likelihood and impact. The maturity model measures strength based on the degree to which the documented evidence supports that controls were designed effectively and are functioning accordingly. This is accomplished when the internal auditor reviews supporting documentation and draws reasonable conclusions about their effectiveness. Auditors rate each control on the scale (see "Degree of Evidence Rating" on page 51).

To illustrate how the degree of evidence is measured, assume an internal auditor is reviewing a control that requires anti-corruption training to be provided to all employees in a format consistent with the local languages in all business units. The business operates in Germany, Greece, Spain, and the U.S. To facilitate training, management provides PowerPoint slides in English, German, and Spanish, but

VISIT InternalAuditor.org to view an example of an assessment based on the anti-corruption maturity model.

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

ANTI-CORRUPTION MATURITY MODEL COMPONENTS

COMPONENT	ANTI-CORRUPTION CONTROLS	
Oversight	» Board oversees the program. » Senior executive is accountable for entity-wide implementation. » Periodic reporting to board on program's effectiveness occurs.	» Program is externally verified. » Authorization and approval thresholds are in place. » Subsidiaries certify to implementation. » Survey verifies employee awareness.
Resources	» Human, financial, and technological resources are sufficient and commensurate with the organization's size and complexity. » Board verifies that resources are sufficient.	» Anti-corruption program has a separate line item in the corporate budget. » Allocation is risk-based.
Risk Assessment	» Is commensurate with size and complexity of the organization. » Includes all drivers of corruption risk. » Is conducted at least annually.	» Includes all foreign operations. » Requires training for participants. » Includes participants from high-risk countries and processes.
Policy Statements	» Set zero tolerance of bribery/corruption. » Establish roles and responsibilities throughout the organization. » Prohibit facilitation payments. » Are translated into all applicable languages. » Are easily accessible by all employees. » Address gifts, entertainment, and charitable and political contributions.	» Are communicated to significant third-party business partners, who certify to their compliance. » Require verification of understanding and compliance. » Prohibit retaliation against issue-spotters.
Third-party Due Diligence	» Search for politically exposed persons. » Search for previous corruption investigations or prosecutions. » Verify legitimacy of charities. » Include in merger and acquisition due diligence.	» Use third-party experts to assist in due diligence activities. » Perform substantive procedures in high-risk locations and processes.
Controls and Monitoring	» Financial system includes transaction-level authorization and segregation of duties controls. » Access to set up new customers and vendors is limited. » High-risk and unusual transactions are continuously monitored.	» Exception reports are reviewed and resolved shortly after report is generated. » Procedures ensure there are no off-the-books transactions. » Controls over setting up foreign bank accounts are in place.
Training	» Provided to all employees, board members, and significant business partners. » Translated into all applicable languages. » Reinforced periodically. » Is tested to verify understanding of the compliance program.	» Addresses gifts, entertainment, and charitable and political contributions. » Includes examples of red flags pertinent to the organization. » Addresses facilitation payments and commercial bribery.

CAEs can help organizations manage corruption risk by assuring an investigative process is in place, according to The IIA Audit Executive Center's What CAEs Can Do to Fight Commercial Bribery.

DEGREE OF EVIDENCE RATING

RATING	QUALIFICATION
0	**No evidence that a policy or control exists.**
1	**Policy documents exist, but there is no evidence that the procedures outlined in the policy documents have been implemented or have taken place.** For example, the policy calls for employees to sign ethics statements, but there is no documentation that they were signed.
2	**Policy documents exist, but evidence supporting the control is inconsistent in either the manner in which the control is applied or documented** (i.e., activity occurs some of the time, but not most or all of the time).
3	**Policy documents exist and documented evidence supports that the control activities have occurred;** however, there are opportunities to improve consistency of application, enforcement, or documentation (i.e., activity occurs most of the time, but not all of the time).
4	**Policy documents exist and there is clear evidence that the control activities are consistently applied and documented.**

it was not able to translate the slide decks into Greek. The auditor rates this control "3" and recommends that the organization translate the training slides into Greek and include them in the online training software.

The process continues until all controls have been assessed. If there is not a control for a significant risk, that attribute receives a zero score.

This methodology gives the internal auditor a deliverable that can provide management with a better picture of the strengths and weaknesses of its anti-corruption controls than it would have using a pass/fail method. That method would have failed the training control in the PowerPoint example because not all employees received instruction in their local languages. Using Excel to document and rate controls enables the auditor to easily tally ratings by component into an assessment scorecard.

TALLYING THE SCORECARD

After internal audit has assessed all of the controls in the respective components and established the degree of evidence, it should determine the effectiveness of the individual components and the overall compliance program by tallying the degree of evidence scores by component. The company for which this model was designed identified 107 compliance controls. The maximum score that can be attained for each component is the number of controls that were assessed multiplied by four, the highest degree of evidence rating. The actual score achieved in each component is divided by the maximum attainable score to arrive at the percentage score. This percentage score will be used to establish the level on which each component will be rated in the model. For example, the oversight component contains 17 controls for a maximum score of 68. If the component's actual score is 47, then its rating is 69 percent.

EVIDENCE OF EFFECTIVENESS

A capability maturity model can be an effective tool for assessing the strength of an anti-corruption compliance program. The evidence-based methodology provides internal auditors who are assessing these programs unambiguous results based on empirical evidence rather than results based on subjective perception. It also provides management an easy-to-read summary that executives can use to identify improvement opportunities for the anti-corruption program as well as a methodology that can be easily repeated in future years. Ia

PAUL J. MORRISON, CPA, *is a director, internal audit services, at Saltchuk/Tropical Shipping in West Palm Beach, Fla.*

Craft Our Role

The 2016-2017 chairman of the North American Board, ROBERT KULING, encourages internal auditors to create the role for themselves that is best for both the organization and their own personal development.

My journey into internal auditing began in 1993, quite by accident, when I was offered a position as a value-for-money auditor with the provincial auditor's office in the Canadian province of Saskatchewan. Twenty-three years later, the business world and the practice of internal auditing have altered beyond recognition—but the fundamental principles remain the same. A mixture of digitization, globalization, regulation, corporate governance reform, and new business practices has changed what organizations want and need from internal audit. And that change is ongoing. Internal audit now has more access to the board in many organizations and is looked at to provide not just hindsight and

Photographs by Colin Way

"Internal auditors can take the first step in crafting their role by developing their business acumen."

insight, but also foresight. To do that, auditors need to combine traditional technical skills with heightened communication and leadership capabilities.

These new pressures are challenging for internal auditors, but they also offer us great opportunities to serve organizations in ways that deliver real benefits. In that context, the theme for my year as chairman of The IIA's North American Board is "Craft Our Role." It is a professional imperative that internal auditors use creativity, ingenuity, and resourcefulness to create the role that is best for both our organizations and our own personal development and fulfillment.

TAKE A BROAD VIEW

There are great internal audit departments and practitioners throughout North America — I have had the pleasure of meeting and working with many of them during my career. However, all too frequently, internal auditors define the initial scope of their work narrowly and, as a result, limit their contributions to the organization. We need to think strategically about what our impact and value could be and use imagination, personal bravery, and professional development to craft our ideal role.

This approach requires a strategic and business-focused type of thinking. Most auditors coming into a new organization rely heavily on their traditional tools and techniques. They instinctively look at what they can audit and apply their competencies to the best way of getting it done. But that is only part of the equation. The internal auditor's potential role and impact is wider and requires a different, more fundamental way of thinking about what it means to provide business value.

While it is crucial to have technical audit skills, the first step for an auditor coming into a new position should be to learn about the business — to understand the performance drivers, strategic opportunities, and key risks the business faces. I suggest starting with core disclosure documents — for example, annual reports and 10-K filings — industry studies, and relevant business literature. Technical audit skills kick in naturally when the auditor starts working on specific projects; business knowledge does not.

In addition, auditors who are approaching the job from the point of view of what is auditable from a controls standpoint risk missing the bigger picture — the structure, culture, and operating philosophy of the departments and functions they are assessing. It can be the difference between checking and approving transactions in an accounts payable ledger and stepping back to understand the effectiveness of the environment, people, systems, and processes in which those transactions are being handled. Many of today's corporate breakdowns happen because the culture around perfectly good controls is faulty. Too few auditors take the time to consider the broader organizational context of the work they are doing.

HARVEST THE KNOWLEDGE

The term *craft* suggests something that is handmade and original that takes time and patience to master. One enriches one's own craft with regular practice, care, constant improvement, and attention to quality. Crafting an internal audit role involves working with other subject matter experts, not just other internal auditors, to increase knowledge and acceptance.

Internal audit's often narrow focus fuels perceptions across the organization that internal audit is too detail-oriented and analytical. Crafting a broader role — from a controls checker to a business adviser — forces internal auditors to understand the control environment and

"The objective is to harvest the **knowledge** and **intellectual capital** readily available in our organizations to make us more business savvy auditors."

focus on the bigger, more important risk issues facing our organizations.

Internal auditors can take the first step in crafting their role by developing their business acumen. The need for this could not be better stated than it was in the most recent IIA Research Foundation Global Internal Audit Common Body of Knowledge study in which 77 percent of stakeholder respondents indicated that "strong relationships with operational and functional leaders" is the top strategy to prioritize competing demands for internal audit.

The starting point is identifying those individuals who drive various business functions and have the inclination to educate internal audit in a practical manner (not all do). Auditors need to build up a network of people who can educate them about the business in a safe, collegial manner—over lunch or a drink after work. It takes courage to introduce yourself and declare your lack of operational knowledge, but it is well worth the effort. The objective is to harvest the knowledge and intellectual capital readily available in our organizations to make us more business savvy auditors.

Let's take an internal auditor who works for a trading organization, for example. The first step would be to find a few traders who can explain in simple terms what they do and how they do it. The traders need to understand it's a safe "nonaudit" conversation so they can be as open and informative as possible. The auditor can supplement this information with insights from relevant professional bodies, regulators, service providers, and other groups to provide a broader perspective on how companies successfully trade their products or commodities. Collectively, this gives the auditor a solid understanding of how trading works and a reasonable basis to think through benchmarking and best practice considerations. The auditor should be able to develop a clear sense of how well the business is performing in relation to others in the marketplace and where the potential weaknesses might be. The key is to learn enough to ask the right questions when the time comes to start auditing.

BUILD ALLIANCES

CAEs should forge meaningful alliances across the organization to craft

2002
Vice President Programs, IIA-Saskatchewan

2003
President, IIA-Saskatchewan

2004
CAE, Precision Drilling

2004
IIA District Representative

2006
Member, IIA Ethics Committee

2008
Chairman, IIA North American Nominating Committee

2013
CAE, Viterra

2013
IIA North American Board/ Canadian Board

2014
Partner, Enterprise Risk Services, Deloitte

2016
Chairman, IIA North American Board

2001
CAE, Saskatchewan Wheat Pool

1995
C$
Manager, Corporate Audit, Farm Credit Canada

1993
Value-for-money Auditor, Saskatchewan Provincial Auditor's Office

MY CAREER PATH

their role and maximize internal resources. When I was the director of audit services at Precision Drilling, it became clear that a certain management group had the most pervasive influence over day-to-day business operations. They drove the culture and operating practices of the company at the field level for everything from people to purchasing to safety. In total, the company had around 24 of these field superintendents. I made it a key objective on my performance plan to be on a "first name" basis with all of these individuals. This was not easy because these superintendents were spread across Western Canada. However, building relationships with this group paid off with more efficient and timely audits.

It often requires ingenuity and persistence to extend the CAE's knowledge of the business. In this case, the field superintendents respected me for taking time to understand their challenges and did not view me as another visitor from "head office." The lesson here is that internal auditors have to make a conscious decision to get out of the office and go to corporate, social, charitable, or networking events to build networks. We need to show an interest and experience the environment. This is all part of crafting our role and creating a positive personal brand—our "persona"—within the organization.

These efforts also give internal auditors a keen sense of the culture and management style in the department, division, or unit they are auditing. We may not get this insight from the traditional audit program. Being culturally sensitive makes the people we are auditing more comfortable with sharing information. The benefit is more meaningful and substantial audit deliverables. Having tangible examples of the soft controls also means more relevant information for the auditor to understand, synthesize, and effectively communicate.

PRACTICE COMBINED ASSURANCE

At the forefront of the profession's challenges today is internal audit's relationship with the second line of defense. It is critical for auditors to forge appropriate and mutually beneficial relationships with the risk management and compliance functions. When internal auditors reach out, we should be describing the benefits of combined assurance or integrated assurance. Internal audit can advocate and implement coordinated approaches to achieve numerous benefits, including common terminology, coordination of resources to reduce audit fatigue, consolidated reporting, and potential reduction in assurance costs.

The reality is that people are protective of their own turf. Internal auditors should use creativity and

As I assume leadership of the North American Board for 2016-2017, I feel a deep sense of pride both as a Canadian, the first to hold the post, and as a Deloitte partner. The support from the firm for me in this role has been excellent. Special thanks to my wife Verna who has been my adviser and confidante and who, along with our three children, has been so supportive, especially when I was away on all those IIA trips.

In addition to carrying out the strategies and tactics outlined in the North American Strategic Plan, my priorities as chairman are twofold. First, I would like to see the skills and expertise of North American members increase through certification and membership in our specialty centers. Second, I would like to

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

SOURCE: WHEAT, JUSTONE/SHUTTERSTOCK.COM: MAPLE LEAF, FMSTOX/SHUTTERSTOCK.COM: OIL WELL, POPCIC/SHUTTERSTOCK.COM: SCALES OF JUSTICE, PAUL CRASH/SHUTTERSTOCK.COM: FARM, BIORAVEN/SHUTTERSTOCK.COM; GRAPH, GRAPHIXMANIA/ SHUTTERSTOCK.COM

drive continual improvement of our advocacy efforts, particularly with CAEs and audit committee members to ensure internal audit is embedded (and funded) in the governance structure of organizations.

relationship building tactics to reach out to the second-line-of-defense functions. We can reduce inefficient communications by having these functions share reports and dashboards, getting access to databases, and attending periodic meetings. A regular cadence for information sharing will clarify audit objectives and strategies and reduce confusion and overlap. Internal audit can incorporate the second-line-of-defense teams as part of its information gathering and risk monitoring capabilities.

The CAE also can make up hybrid teams of audit and nonaudit staff to expand resources where the project allows. In one organization where I was the CAE, we had a major inventory challenge in global operations. To execute the project within a tight time frame, I doubled the size of my audit team of 12 auditors by working with the finance organization to obtain additional qualified individuals to ensure appropriate coverage. Internal audit took the leadership role, and we completed the project in a matter of weeks, resulting in significant changes to inventory management practices and millions of dollars of inventory adjustments.

Another example comes from my time at Farm Credit Canada—an agricultural lending organization. For every audit, we included a risk management officer as a secondee on the field audit team. The program was so popular that the number of individuals wanting to join audit projects exceeded our number of planned audits. This arrangement worked because our risk management partners were able to improve their business knowledge and understanding of local operations.

Maximizing external resources is a unique challenge for CAEs who are usually working under budgetary constraints. When I was a practicing CAE, I always battled to ensure my budget included amounts for cosourced audit projects. There were always two potential project streams to deploy these resources—to build methodology and knowledge transfer to the core audit team or for standalone projects that are best planned and executed by an external service provider.

In my conversations with CAEs over the years, I was constantly perplexed that outsourcing budget dollars, although available, were not always used. Coming under budget is not necessarily a good result for the internal audit function. The outsourcing budget should be used for risk-based projects and emerging needs that cannot be performed using the existing audit team's skills.

CRAFT A CAREER

Crafting one's role also means maintaining and continually upgrading one's technical expertise. The foundational building block is the Certified Internal Auditor designation—the auditor's "license" to perform professional internal audit work. But why stop there? If auditors work in specialized fields, they should consider taking IIA or other post-certificate qualifications to boost their knowledge. For example, my Certified Quality Auditor designation from the American Society for Quality has served me well over the years. Internal auditors should think creatively about the career path they want and challenge themselves to continually upgrade their technical competencies to grow inside or outside the profession.

I challenge North American members to take on a new IIA certification and professional training outside their comfort zone this year. Resolve to hone your craft, build your networks, and maximize resources. A good craftsman or craftswoman earns the confidence of customers with knowledge, resourcefulness, versatility, and most importantly, customer service. Ia

ROBERT KULING, CIA, CRMA, CQA, *is a partner, Enterprise Risk Services, with Deloitte & Touche LLP in Calgary, Alberta.*

Fraud
and related-party transactions

James A. Bailey

Internal auditors can identify red flags and reduce the risk and impact of related-party fraud.

Individuals who use their positions to secretly benefit themselves at the expense of their employers betray the trust of the organizations that employ them. Often, these transgressions take the form of undisclosed related-party transactions, where the individuals who approve the transactions for their organizations also benefit personally from them.

Internal auditors need to identify the red flags of related-party loans, sales, and purchase transactions that indicate fraud (see "Red Flags of Related-party Transactions" on page 61). The case studies herein illustrate common methods used to commit various frauds. By identifying the red flags in these cases, internal auditors can improve their ability to recognize related-party fraud risks.

LOANS

The vice president of finance at a service company borrowed US$50,000 from the organization. The note states that it is a zero-interest loan with no collateral or due date. Accounting records and financial statements present the loan as a regular note receivable without disclosing the related-party nature of the note. The vice president also used her position to make the company a guarantor on one of her other personal loans.

Key risks in related-party loan transactions include:

- Providing loans to senior management, other employees, or board members at below-market interest rates or under terms they could not get in the marketplace.
- Failing to disclose the related-party nature of the loan.
- The organization providing guarantees for private loans made by employees or board members.

In all of these risk areas, the favorable terms benefit the employee at the expense of the organization.

Internal Audit Procedures To identify undisclosed loans to senior management, board members, and employees, the internal auditor could search for related-party loans using data analysis to compare the names on all notes receivables and accounts receivables with employee names from payroll records and board member names from board minutes. If a match occurs, the auditor should assess whether the related-party transaction was appropriately authorized and

ILLUSTRATION: FRANCESCO BONGIORNI

disclosed in the accounting records and financial statements.

Auditors also could search for undisclosed related-party loans by examining the interest rate, due dates, and collateral terms for notes receivables. Notes receivable containing zero or unusually low interest rates, or requiring no due dates or insufficient collateral, may indicate related-party transactions. The internal auditor also should examine advances made to customers or others who owe money to the organization. Organizations generally do not advance money to others who owe them money unless a related-party relationship exists.

SALES

A sales agent for a manufacturing company sold a significant amount of goods at a substantial discount to XYZ Supply, a company he owns but has not disclosed the conflict of interest. XYZ Supply, in turn, sold the goods at market rates, thereby providing him with a profit. XYZ returned goods it was unable to sell months later for reimbursement. XYZ did not pay accounts receivable for several purchases, and the sales agent persuaded the credit department manager to write off the related receivables.

Key risks for related-party sales include employees:

- Selling products or services significantly below market price or providing beneficial sales terms that ordinarily would not be granted to arms-length customers.
- Inflating sales for bonuses or stock options using related parties to perpetrate the scheme. Either a sale really has not taken place because the goods were not shipped or there was an obligation to repurchase the goods sold so the sale was incomplete.
- Approving excessive sales allowances or returns as well as accounts receivable adjustments or write-offs for related parties.

Organizations should maintain written policies and procedures for related-party relationships.

In an effort to cover up the related-party transaction, employees may deny auditors access to customers to impede them from acquiring audit evidence concerning the related-party relationship.

Internal Audit Procedures Internal auditors should perform analytical procedures to compare price variations among customers to identify those who pay significantly below the average sales price. Auditors also should identify any customer who pays prices that differ from the approved price sheet. Customer contracts should be analyzed for unusual rights of return, obligations to repurchase goods sold, and unusual extended repayment terms. Analytical procedures to identify customers with excessive returns, sales allowances, account receivable adjustments, or write-offs also should be performed. Any variances in these areas could indicate undisclosed related-party transactions.

Data analysis can be used to compare employee addresses, telephone numbers, tax identification numbers, and birthdays with customer addresses, telephone numbers, tax identification numbers, and company organization dates. When creating a shell company, many individuals use their own contact information for convenience and their own birth date as the organization date because it is easy to remember. Any matches could indicate a related-party association and should be investigated.

PURCHASES

A purchasing agent for a manufacturing company buys goods for his employer from a company he secretly owns, ABC Supply. For many of the purchases, the prices significantly exceed normal market prices, allowing the purchasing agent to make a personal profit on the difference between what his company pays for the items and what he charges his employer. For other purchases, the product quality is inferior for the price paid because he purchases poor quality goods at a low price, then sells them to his employer at market rates, allowing his company to profit from the transaction.

Key risks for related-party purchases are:

- Paying prices significantly above market for goods or services.
- Receiving significantly below average quality goods or services that are purchased at market prices for high-quality goods or services.
- Never actually receiving the purchased goods or services.

Internal Audit Procedures Auditors should compare cost variations among vendors to identify those whose costs significantly exceed the average cost. For identified variances, auditors should discover why the cost variations occurred to assess whether a related-party relationship exists.

Similar to the audit of customers, auditors should compare the employee's address, telephone number, tax identification number, and birth date to vendors' information to see if a relationship exists. Auditors also should assess the use of sales intermediaries for products they can purchase directly from the manufacturer at lower costs.

Initial detection of occupational fraud schemes is most common by tip (39.1%) followed by internal audit (16.1%), according to the Association of Certified Fraud Examiners' 2016 Report to the Nations.

RED FLAGS OF RELATED-PARTY TRANSACTIONS

When reviewing related-party transactions, auditors should be aware of the red flags that may indicate fraud is taking place.

Loan Frauds

- Loans to officers, board members, or employees.
- Interest-free loans.
- Insufficient collateral for loans.
- Loans without fixed repayment terms.
- Loans to parties who cannot repay.
- Providing funds to pay uncollectable loans or receivables.
- Inappropriate guarantees of personal loans.
- Accounting records and financial statement receivables and financial statement disclosures that fail to disclose the related-party nature of the loans.
- Denied access to borrower to acquire audit evidence.

Sales Frauds

- Sales prices significantly below market prices.
- Sales prices below market to sales intermediary with no apparent business purposes.
- Unusual rights of return.
- Obligation to repurchase goods sold.
- Unusual extended repayment terms.
- Excessive sales allowances or returns for a customer.
- Bill and hold sales.
- Unapproved or undocumented accounts receivable adjustments and write-offs for a customer.
- Denied access to customers to acquire audit evidence.

Purchasing Frauds

- Costs significantly above market prices.
- Paying premium prices for generic products.
- Costs above market from a sales intermediary with no apparent business purpose.
- Unusually large amounts of usage and scrap in production due to faulty materials.
- Denied access to vendor to acquire audit evidence.

FINDING PROCESS FAILURES

In reviewing their organization's documentation, internal auditors may find that the organization does not have in place any policies or procedures prohibiting related-party relationships or transactions without prior approval. The organization also may not provide training to employees around related-party relationships and transactions, or require employees to certify whether they are involved in any conflicts of interest with the organization.

Organizations should maintain written policies and procedures defining the process for obtaining approval for related-party relationships and transactions. Key risks exist if:

- Written related-party policy and procedures are nonexistent or insufficient.
- Employees are not required to certify regularly whether they have a conflict of interest.
- Related-party transactions are not approved in accordance with established organizational policies and procedures.
- Related-party transactions are approved with exceptions to organizational policies and procedures.

Internal Audit Procedures The internal auditor should review approved related-party policies and procedures documentation. If related-party policies or procedures don't exist or if they don't sufficiently mitigate the risk of unauthorized or inappropriate related-party relationships or transactions, the auditor should consult with senior management and the board, if necessary, to develop appropriate policies and procedures.

Auditors also should review conflict of interest statements. If an employee documents a conflict of interest in his or her statement, the internal auditor should assess whether the conflict of interest was appropriately authorized and whether the process recognizes and discloses conflicts of interest.

Board minutes should be reviewed for authorization of related-party relationships or transactions conducted by or on behalf of senior management and board members. Auditors also should review documentation of senior management approval for related-party relationships or transactions of non-senior management employees. While reviewing this documentation, internal auditors should assess whether the organization made exceptions to its written policies or procedures during the authorization process. If exceptions were made, the auditor should assess the business purpose and reasonableness of the exception.

COORDINATION

To minimize duplication of effort and to ensure appropriate coverage of

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

related-party risks, the CAE should coordinate activities and share information about those risks with external and internal service providers (see IIA Standard 2050: Coordination). Independent auditors generally are required to consider related-party risks when conducting audits. For example, the International Federation of Accountants' International Standard on Auditing 550 states the independent auditors' responsibilities to specifically address related-party transactions and relationships.

In the United States, the Public Company Accounting Oversight Board's Auditing Standard (AS) 18 requires independent auditors to evaluate related-party relationships and transactions (AS 18 will be renumbered as AS 2410 effective Dec. 31, 2016). By working with the independent auditors, internal auditors could help identify related-party risks that may have a material effect on the financial statements and related required disclosures, while at the same time identifying related-party risks that may fall below the threshold but are still significant to the organization.

The CAE also should consider government regulatory or contractual requirements that may prohibit certain types of related-party transactions or relationships. Internal auditors should work closely with their organization's compliance, risk management, and legal departments to identify related-party risks and assure that these risks are being monitored and mitigated appropriately.

REDUCING RISK

Internal auditors can uncover undisclosed conflicts of interest by recognizing red flags associated with related-party relationships and transactions. Where red flags exist, internal auditors should assess the nature of the transactions and ascertain whether the related-party transactions were authorized appropriately. By discovering unauthorized related-party transactions and assessing related-party policies and processes, internal auditors can identify deficiencies and recommend policy and process improvements to reduce the risk of future unauthorized related-party transactions and relationships. Ia

JAMES A. BAILEY, PHD, CIA, CPA, CFE, *is a professor of accounting at Utah Valley University in Orem.*

Governance Perspectives

BY JJ JENKINS EDITED BY MARK BRINKLEY

COMMUNICATING RESULTS

Sharing audit observations is one of the most important tasks auditors perform.

To maximize its value to the organization, an internal audit should not only identify issues — it also needs to elicit support and action on recommendations. Internal auditors can ensure this occurs, as well as improve their relationship with management, through appropriate communication of audit results.

In fact, the communication of internal audit observations presents many opportunities and should be one of the most thoughtful tasks an internal auditor performs. That isn't to say that audit planning, scoping, and testing are not important, but to achieve the greatest value from the work performed in those phases, the outcome needs to be communicated to the appropriate audience in a way that allows them to understand the results, appreciate the significance of the issue, and take action. Communicating internal audit results is significant enough that the *International Standards for the Professional Practice of Internal Auditing* (*Standards*) has an entire series dedicated to it (see Standard 2400: Communicating Results).

The benefits of communicating results go beyond getting to wrap up an audit and informing management of the need to move forward with issue resolution. When handled appropriately, communication of audit results to management can help enhance rapport, even if the relationship was stressed during the audit. Additionally, communicating results can enhance internal audit's reputation with the audit customer and beyond by showing that the auditor understands the business and legitimate risks and is looking to provide meaningful recommendations.

There are several considerations to keep in mind when determining how best to communicate audit observations.

Make Sure the Observations are Correct While this seems obvious, issues are not always validated before they are communicated to management. Having an audit observation challenged and not being able to support its validity can harm internal audit's ability to convince management to take action on legitimate issues and can significantly harm internal audit's reputation. When new information is presented that changes the audit results, the auditor should be able to identify why internal audit did not have the information before the point of communicating the results. The auditor should give management credit for providing the new information, note why the information was not known, and adjust as necessary.

Plan the Timing of Issue Dissemination Management needs to know about observations as soon as possible, but not so early

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

that the auditor cannot support the issues identified. This is a balancing act and needs to consider each manager's potential actions when receiving the information. Some managers will immediately react, regardless of the significance of the issue or their preparedness to resolve the issue, which may or may not make sense, depending on the issue's nature. Considering what they know about managers and their temperaments before presenting issues can help auditors present appropriately and at the right time. The one constant: Surprising management with all issues at the end of an audit is damaging to the auditor–management relationship and to gaining management's support for audit's efforts.

Write in Clear Prose It is important not to soften an observation to the point that a reader does not realize the importance of, or value in, remediation. On the other hand, a report written in a strictly negative tone also may limit management's engagement in the observations and desire to work with internal audit to resolve noted items. There is more than one way to say something, and typically there is a way to say something so it is accepted and another way to make people defensive. While some may see this as being political, a lack of appropriate wording may result in the recipient not seeing the value in internal audit's work. If the goal is to create action to mitigate risk and resolve concerns, the specific words internal audit uses are important.

Exercise Diplomacy Internal audit can improve its relationship with management even when communicating observations by exercising diplomacy. For example, taking the opportunity to acknowledge the audit customer's team achievements or its efforts to mitigate significant risks shows management that internal audit is not only focused on the identification of issues.

Understand the Business and Associated Risks Internal audit's customers understand their business. They know what their department does, and they have considered the risks related to their function. Therefore, if internal audit cannot show that it also has a handle on each of these items, it may be hard for auditors to communicate observations in a way management is willing to listen to or can understand.

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

One of the quickest ways to lose management's respect is to make it clear that internal audit does not understand what it has been auditing. The answer is to take the time to learn the business, processes, and risks associated with the audited area.

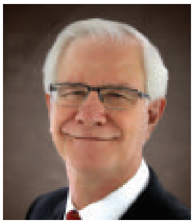
Focus on Legitimate and Reasonable Risks Not every risk is a high risk. Not everything needs to be considered at the greatest possible failure. For example, many auditors identify when there is a lack of policies and procedures. While it is reasonable to notify management that it does not have the appropriate documents to support its processes, it does not mean the department will ultimately collapse without them. The department has probably operated that way for years and could likely operate for a considerable time without it actually creating a problem. That said, the issue should still be identified, but the internal auditor should do it in a way that indicates he or she understands the level of risk it is truly causing and the benefit of continuity that policies and procedures can provide a department.

If tense situations never arise, internal audit is not doing its job.

Internal auditors can actually enhance their reputation with management while working toward remediation of issues. There will be tense situations and disagreements; however, if those situations never arise, internal audit is not doing its job. On the other hand, the internal auditor role is not automatically in conflict with the client — everyone is working toward the same goals of ensuring mitigated or appropriate risk levels, adequately controlled processes, and a successful organization.

JJ JENKINS, CIA, CRMA, *is director of internal audit at CareSource Management Group in Dayton, Ohio.*

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



BY J. MICHAEL JACKA

CANARY IN THE ORGANIZATIONAL COAL MINE

Internal audit serves as a key warning indicator, but only when stakeholders truly appreciate its value.

In the 1980s, I worked for one of the most ineffectual managers of all time. Everyone who served on his audit team struggled to understand why executive management never took action to address his failures. Over time I learned that part of the reason was that some executives assumed the department functioned effectively. Audit reports never included any significant issues, so they thought internal audit must be doing a great job. The experience taught me a valuable and interesting lesson about audit departments.

When executives do not have a clear understanding of the role and impact of an effective internal audit function, those executives often believe that a successful audit team is one that causes no problems. There are no waves, no headaches, no imbroglios, no brouhahas—so internal audit must be doing its job.

But there is something even more insidious within this perception. Without an understanding of what an effective audit function does, stakeholders will not recognize how internal audit's failure to warn them appropriately might hasten organizational harm.

Internal audit is the canary in the organizational coal mine. Just as miners used canaries to provide early detection of lethal conditions, internal audit provides stakeholders with early warnings of an organization's potentially lethal actions. But the canary is only effective when the miner knows what to expect. And when stakeholders are not educated—when the negative impacts of an ineffective audit department are unknown—those stakeholders will go blithely forward with a false sense of security.

It seems that, when a failure occurs, more people are asking "Where were the auditors?" That is a good start. But the question should be asked after every single incident. The inquiry alone reveals an increased understanding of our impact and potential.

The profession has made great strides since my experiences in the 1980s. Internal audit is seen by many organizations as an integral part of the governance structure. (As evidence of how far we've come, the word *governance* was seldom bandied about in the 1980s.) And most executives who now deal with internal auditors understand the importance and impact they can have on the success of the organization. But we are not quite there yet.

When internal audit has a strong presence in the organization and provides executives with valuable insights, those executives appreciate the input. But when internal audit drops off the radar, executives become overwhelmed by everything else on their busy agendas, losing sight of internal audit's important role.

Miners felt the absence. If a canary wasn't around, they knew they needed to find one. Do executives look around for that security when internal audit doesn't seem to be present? Or to put it another way, would they know they should miss you if you were gone? 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

CARE AND FEEDING OF THE COMPANY'S CULTURE

Two experts discuss internal audit's role in ensuring a healthy organizational culture.

JASON PETT
U.S. Internal Audit Solutions Leader
Pricewaterhouse-Coopers

SANDY PUNDMANN
U.S. Managing Partner, Internal Audit
Deloitte & Touche

Why audit organizational culture?

PETT It wasn't only through missing or weak controls and processes that the recent credit crisis and the Forex and LIBOR scandals crystallized. They were partially attributable to poor decision-making, a lack of integrity and ethical behavior, and a failure to diagnose and correct poor behavior and culture. In addition to more traditional auditing, there is a need to audit culture to establish the root cause of poor behavior and stop it quickly. Internal audit, through its work and focus on audit results and cultural themes, can provide the board and executives some assurance and a point of view on the state of organizational culture and the responsiveness of the organization to acknowledge and address cultural issues.

PUNDMANN The tie that binds in many corporate funerals is an unhealthy organizational culture. While we may attribute organizational failures to things like fraud, poor leadership decisions, and other such symptoms, culture is really at the crux. Auditing culture can reveal if there's a gap between perceived culture and what employees and others report as reality. When you're relying on internal and external third parties to act in a consistent, ethical manner on your behalf, it's worth examining.

What are the characteristics of a healthy culture?

PUNDMANN Healthy organizations have guidance on norms and expectations. Tone at the top in healthy cultures is communicated and espoused firmwide for the long term. Healthy cultures enable broad thinking and appropriate risk taking, without focusing myopically on the next quarter's results. It sounds simple enough, but it's actually quite rare.

The hallmark of an unhealthy culture is the "no bad news" approach. If people face retribution for raising issues that might be contrary to expected outcomes, why raise a hand? Unhealthy organizations also are the most resistant to culture audits.

PETT A healthy culture starts with clarity and transparency at the top. When leadership clearly sets the organization's vision and values, and reinforces them with both consistent communication and a complementary measurement system, expectations around culture are clearly established. These messages should promote professional skepticism and encourage staff to speak up with autonomy and confidence, without concern about impact on personal reputation and perception. A healthy culture means the board and management hold a well-balanced short- and long-term view on an organization's strategy and bottom line. Collectively, these characteristics will contribute to an organization's long-term success.

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

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

How should auditors go about auditing culture?

PETT Culture is the DNA of an organization. Additionally, there are multiple subcultures that exist across an organization. The key is to determine where the real hot spots are, such as the teams, divisions, management lines, and activities that potentially present high-impact culture risk. It is therefore important to carry out a culture risk assessment. Auditors should draw on their knowledge and experience gathered through their work and use key business and operational data points that can provide behavioral indicators. Once key culture risk areas are identified, auditors must adopt a methodical approach to consider these areas during all of their audit activities and assess and test the root cause of issues identified during audit activity to determine if cultural concerns are at or near the core of the issue. They should look beyond the control or process concerns and ask the question, "Is the root cause behavioral or cultural?" This is one strategy to embed cultural auditing into the day-to-day audit activities of the department.

PUNDMANN While some may use the words *testing* and *monitoring* interchangeably, they should be separate and applied to any audit of culture. Start with a risk assessment to see what an organization is already doing to understand, communicate, and shape its corporate culture. To test whether existing efforts are effective, talk to senior management, the audit committee, and other leaders to get their take. Then, compare the assessment from leadership with feedback you receive from middle management and employees to identify gaps between leadership understanding and day-to-day practice. Consider starting small, perhaps by auditing the culture of a business unit seen as healthy. Then analyze the gap between the healthy business unit with those that aren't seen as positively. Of course after various cultural gaps are identified, be sure to monitor efforts to close them. Software solutions can help auditors identify cultural strengths and gaps, and later monitor progress of efforts to enact change.

Why don't more organizations audit culture?

PUNDMANN Unlike so many things we audit where we know what the control is and whether things varied from it, auditing culture is not so clear-cut. It's very subjective and hard to evaluate. Within some organizations, culture can differ by business unit, subsidiary, or just one team. But having the ability to honestly communicate with the board, the audit committee, and corporate leaders about corporate culture can be a true strategic enabler.

PETT Culture and behavior to many people are often nebulous concepts that are viewed as difficult to audit credibly using traditional methods. This combined with historically theoretical culture debates and points of view presented by industry, organizations, and regulators—that have not pointed to culture as a material root cause of failing companies—have resulted in organizations not auditing culture in a meaningful way. It would seem there is a change occurring, with culture audits beginning to appear in audit plans.

What skills do internal auditors need to audit culture?

PETT Internal auditors need not only to be controls and business experts, but they also need to have heightened levels of self-awareness and be more sensitive to the emotional drivers of teams, management, and the organizations. They need to understand how poor behavior can adversely impact day-to-day activities within an organization and ultimately its strategic direction. A good balance between left brain thinking—logical, analytical, technical—and right brain thinking—creative, feelings, holistic— is needed. That said, auditors do not need to be psychologists. Instead, more honed soft skills combined with effective communication capabilities will help them engage in credible culture discussions and educate stakeholders on the importance of culture and behavior.

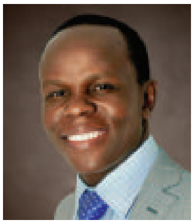
PUNDMANN Culture audits require tenacity, an analytic mind, healthy skepticism, and the willingness to ask for help. In some cases, internal auditors need to persuade leaders when a culture audit is needed—often reaching out of our groups to build consensus. Once the audit is underway, we need to correlate observations of our own with perspectives from various sources, being mindful of information sources and myriad variables that stand to sway discussions. After initial culture audit results are in, internal audit often contributes to efforts driven by talent, compliance, and other groups to help improve challenged areas.

How can a toxic culture change?

PUNDMANN To truly change a culture, you have to take action. Identifying gaps between leadership perceptions and employee realities in corporate culture is one thing. But changing behavior takes time, consistency, and investments from across an organization to improve.

PETT A toxic culture can only be changed if leadership can diagnose it, is willing to act on and remediate the root cause, and can hold accountable those individuals who are causing the toxicity to occur. Boards, executives, and management need to review their measurement systems to ensure they are not running contrary to their desired values, and must showcase that they take poor culture and behavior seriously, continually reinforcing this to ensure they can influence the change they seek. Methods exist in organizations to deal with poor behavior such as private warnings, performance plans, or termination. However, the key is to make the action taken public and link it as a consequence of poor culture and behavior. Ia

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



BY TICHAONA ZORORO

THE VALUE OF CONTEXT

Management's understanding of findings often hinges on how they're framed in the audit report.

In far too many instances, audit reports fall short of providing stakeholders the value-added assessments they require. Issues raised in reports often lack business-relevant context and neglect to offer meaningful, concrete details that help communicate items of importance. Delivery of useful insight that stakeholders can leverage for improvement relies on practitioners' ability to frame information in a way that captures attention and resonates with the intended audience.

There are many opportunities for internal auditors to miss the mark in audit reports. One example of a finding that often falls flat is, "The disaster recovery plan (DRP) has not been tested." Left without context to the business under review, this audit issue does not add value. An examination of DRP should help gauge whether the organization can continue to provide critical services in the event of tragedy. Moreover, criticality of services differs according to the nature of the area under review. Practitioners must detail the significance of each finding according to how it affects the audited business.

Contextualization of key issues helps gain the attention of stakeholders by making these issues more concrete. For example, suppose a bank in South Africa seeks to increase its revenue from ATMs. In the prior year its total revenue from ATM charges was R90 million (US$5.72 million); the board and senior executives seek to increase it to R120 million in the current financial year. At R90 million annually, the average monthly income would be R7.5 million, which translates to a weekly average of R1.875 million. If ATM systems are down for, say, two weeks, the bank will lose income of about R3.75 million. Citing this calculation in a report lends more weight to the finding and places the risk in perspective.

Business metrics should be communicated in a way that delivers impact and provides insight. In the ATM example, referencing instances where ATMs were down during the year, including their effect on fee revenue, would strengthen the audit report. Moreover, failure to test the ATM system for recovery in the current year means a lack of assurance that ATM services will be available continually. The performance objective of increasing ATM revenue to R120 million may be jeopardized, not to mention the negative impact on the bank's reputation and the possible loss of clients to competing banks. Citing each of these points would lend further clarity to the report.

By considering context, internal auditors can help ensure not only that findings point to areas of concern, but that management appreciates their significance. Merely drawing attention to issues differs dramatically from communicating them in a way that imparts urgency and promotes action. Without appropriate context, internal auditors' hard-earned, carefully prepared insights may never translate to results and improvement for the organizations they serve. Ia

TICHAONA ZORORO, CIA, CRMA, CGEIT, COBIT 5 CERTIFIED ASSESSOR, *is an IT advisory executive with EGIT | Enterprise Governance of IT (Pty) Ltd. in Johannesburg, South Africa.*

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

Wolters Kluwer

When you have to be right

TeamMate®

Fraud is rampant.

Waste is costly.

The right tools are critical.

Audit with confidence.

PRINCIPAL PARTNER

Learn more today at:
TeamMateSolutions.com/TheRightTool