Ia
INTERNAL AUDITOR

AUGUST 2017
INTERNALAUDITOR.ORG

Managing and Protecting Data

Tech Expectations of Today's Internal Auditor

Analytics and the Audit Function

New IIA Global Chairman on #PurposeServiceImpact

THE TECHNOLOGY ISSUE

Ia
INTERNAL AUDITOR

AUGUST 2017 VOLUME LXXIV: IV

FEATURES


John Smith, CRMA
Director, Internal Audit
Monroe Manufacturing
1525 West Main Street / Stonybrook, MN

Ia
INTERNAL AUDITOR

AUGUST 2017 VOLUME LXXIV: IV

DEPARTMENTS

ONLINE InternalAuditor.org

The Internet of Risks The rise of connected devices through the Internet of Things creates a multitude of organizational exposures.

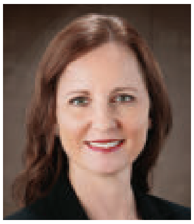
Chairman's Video Watch The IIA's 2017-2018 Global Chairman J. Michael Peppers discuss his theme for the upcoming year, #PurposeServiceImpact.

The Costly Parking Lot Auditors in Canada raise questions about the inflated price of a land deal. Fraud expert Art Stewart explains why.

Repairing the Weakest Link A recent survey says employee actions are at the heart of most cybersecurity incidents reported to insurers.

Find us on Facebook

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



A TECHNOLOGY REVOLUTION

The technology landscape changes at such speed that most of us have trouble trying to keep up. Smartphones, apps, and social media often leave our heads spinning with their constant updates. As soon as you master a newly launched technology, there's another one on the horizon. Imagine the difficulty in wrapping your head around this rapid change at the business level.

Fifty-two percent of business and IT leaders rate their organization's digital IQ—a measure of an organization's capability to get strategic value from technology investments—as strong in PricewaterhouseCoopers' 2017 Digital IQ survey. This is a significant drop from previous years: 67 percent in 2016 and 66 percent in 2015.

While businesses see the value in adopting new technologies, many of them have not adapted quickly enough to keep up with the technology curve. Technology and business are inseparable, so businesses that neglect to embrace this relationship are sure to fail. For internal auditors, that means understanding the evolving risk landscape related to the business and learning to use technology in their work.

"There is no business today that is not driven by data," says Dominique Vincenti, Nordstrom's vice president of Internal Audit and Financial Controls. In our cover story, "In Safe Hands" (page 26), Vincenti says businesses need to fundamentally reassess what data means to their organizations going forward. New laws such as the European Union's General Data Protection Regulation (going into effect spring 2018) will require companies to have more control over what data can be held and how it can be used.

More importantly, the increased risks from ransomware attacks, data breaches, blockchain adoption, the Internet of Things, use of artificial intelligence, and data collection and its ethical use—the list goes on and on—beg the question: Are internal auditors equipped to handle the technology embedded into business practices?

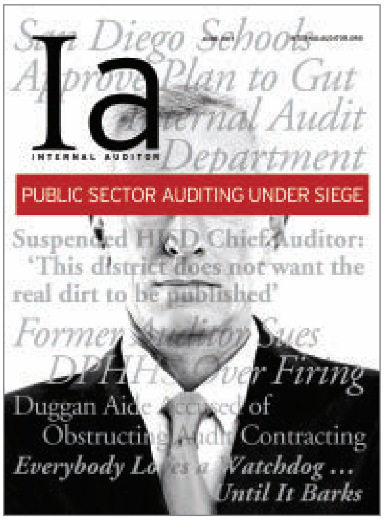
IT expertise among internal auditors is now a general expectation, according to "Great Tech Expectations" (page 32). Author Russell Jackson says today's internal audit new hires who have grown up with smartphones and technology often have more advanced IT skills on day one than their predecessors. Office Depot's Chief Audit Executive Jennifer Goschke stresses that "it's important to have IT subject matter experts on your team to provide the technical chops to be able to go head to head with IT." But while auditors with IT experience are still in high demand, they continue to be hard to find, afford, and retain.

Technology will continue to disrupt and change the business landscape at an increasingly rapid pace—what some futurists call The Fourth Industrial Revolution. One thing is certain: Organizations that resist that change will not survive.

Shannon Steffee

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.



A Thankless Job?

It can be a thankless job to ask difficult questions and deliver unpleasant recommendations in the transparent culture of public organizations. Add to that mix political retaliation for simply doing one's job, which is a sad fact internal auditors are faced with. Audit practitioners in recent retaliation headlines provide both a warning and a level of support for professional auditors to maintain an ethical true course. I agree that it is imperative that we continue to honor The IIA's Code of Ethics when performing audit engagements and hope that by maintaining strong communication with management, as suggested in the article, we can show we support the same goal: effective organizational services.

EMILY KIDD *comments on Russell Jackson's "Under Siege" (June 2017).*

Organizational Watchdogs

Unfortunately, it has been pounded into our heads that we need to change our image from that of "gotcha" or police to a softer persona. As auditors, we are that last defense in making sure that the organization is operating in a way that minimizes risks, safeguards resources, and protects stakeholders. Sometimes the truth hurts, and senior management needs to understand that auditors are there to help keep the organization out of trouble. Given the recent news about organizations—from government to the private sector—getting into trouble, many have asked where the safeguards were. Or, how did this occur without someone raising questions? This is where auditors come in—to be that watchdog protecting the organization when all other defenses fail. After all, would they rather have the auditor identify the problem so the organization can address it? Or would they like the media and outsiders to find out and crucify the organization? I am willing to bet most would choose the auditor option.

FREDRICK LEE *comments on Christine Hogan Hayes' "Internal Audit as Police" ("In My Opinion," June 2017).*

Friend or Foe?

During my last two positions as a chief audit executive, I have reported administratively to the general counsel to avoid reporting to the chief financial officer, who is responsible for the primary areas I have audited. Thankfully, I have not had any serious disagreements with the general counsel on internal audit findings or reports.

MICHAEL PEAK *comments on the Chambers on the Profession blog post, "For Internal Audit—Is the General Counsel Friend or Foe?"*

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

Ia INTERNAL AUDITOR
AUGUST 2017
VOLUME LXXIV:IV

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

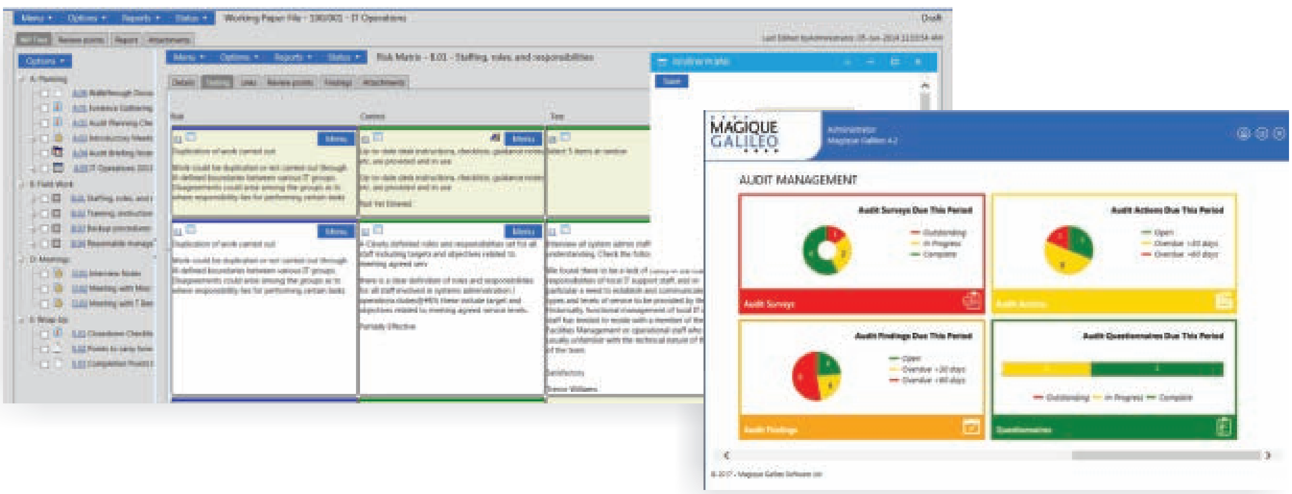
PERMISSIONS AND REPRINTS
editor@theiia.org
+1-407-937-1232; fax +1-407-937-1101

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

MAGIQUE GALILEO

Your Solution to Effective Internal Audit and Compliance

- Galileo is a comprehensive and fully integrated audit and compliance system
- Used by over 200 organizations in over 80 countries catering for teams from 5 to over 1,000
- System can be installed on customer infrastructure or provided as a SAAS hosted solution
- Works with any standard browser on laptop, PC, iPad/tablet and other smart devices
- Implemented and supported by experienced audit professionals



Over 350 standard reports, charts, dashboards and scorecards are provided. The system includes a drag and drop end-user reporting tool and comprehensive analysis tools.

Proactively alerts and prompts all stakeholders with the key information required to objectively assess the effectiveness of the assurance framework.

Integrated
a single integrated system that intelligently combines elements to provide a complete picture

Individual
configured and customized to meet your organization and users' exact needs

Intuitive
easy to use system, liked by users, which evolves and grows with you

Innovative
At the forefront with techniques to improve your methodology, efficiency, delivery and profile

www.magiquegalileo.com
+1 212 220 6709 (USA) +44 (0)20 3753 5535 (UK)

EU takes fraud fight across borders... Fewer women named to boards... Defending against ransomware... Guidance advocates crisis resilience.

Update

THE CYBER READINESS GAP

Organizations may not be prepared for the attacks they're expecting.

The one-two punch of this year's WannaCry and Petya ransomware attacks hit businesses around the world hard before many had their guard up. The emergence of ransomware is a big reason 53 percent of security professionals surveyed report a rise in cyberattacks last year, according to the second installment of ISACA's 2017 State of Cyber Security Study. The 633 respondents to the global survey expect things to get worse this year, with 80 percent saying their organization is likely to experience a cyberattack.

Knowing the threats is one thing—readiness is another. Just 31 percent of respondents say their organization tests its security controls routinely, and 13 percent don't test them at all. Only 53 percent have a plan in place to address ransomware attacks.

"There is a significant and concerning gap between the threats an organization faces and its readiness to address those threats in a timely or effective manner," says Christos Dimitriadis, group head of information security at INTRALOT in Athens, Greece.

Next to phishing schemes, malicious code attacks such as ransomware are the most common threat type, respondents report. Sixty-two percent say their organization experienced a ransomware attack in 2016.

Meanwhile, the Internet of Things (IoT) has supplanted mobile devices as

TOP ELECTRONIC MESSAGE CONCERNS

Financial firms have heightened worries about electronic communications.

Non-email channels
54% in 2017 | 35% in 2016

Understanding new and changing regulations
50% in 2017 | 30% in 2016

Mobile communications devices
50% in 2017 | 23% in 2016

Inefficient supervision process
46% in 2017 | 28% in 2016

Source: Smarsh, 2017 Electronic Communications Compliance Survey Report

IMAGES: TOP, GUVENDEMIR / ISTOCK.COM; RIGHT, BROTHERS GOOD / SHUTTERSTOCK.COM

FOR THE LATEST AUDIT-RELATED HEADLINES follow us on Twitter @IaMag_IIA a primary focus of respondent organizations' defenses, with nearly 60 percent of respondents saying they are concerned about attacks on IoT devices. In part, this shift is because most organizations are using encryption to protect mobile device data in the event they are lost or stolen. Also, respondents report they are more aware of IoT technologies that are deployed in their organization compared to past surveys.

Organizations may be fighting more threats without more resources, the report notes. Growth in cybersecurity spending is slowing, with only half of respondents reporting their budget will increase this year. **– T. MCCOLLUM**

62%

OF U.S. FINANCE EXECUTIVES SAY THE NUMBER AND DOLLAR AMOUNT OF CREDIT CARD CHARGEBACKS HAVE INCREASED SINCE CHIP CARD TECHNOLOGY WAS INTRODUCED IN THE U.S.

64%

SAY THE NUMBER AND DOLLAR AMOUNT OF CARD-NOT-PRESENT (CNP) CHARGEBACKS HAVE INCREASED SINCE THAT TIME.

"As merchants have upgraded in-store payment security measures, fraudsters have flocked to CNP channels – online, mobile, and elsewhere – with stolen payment credentials," says Tom Byrnes, chief marketing officer at Vesta Corp.

Source: Vesta Corp. and CFO Research, Managing the Risk of Fraud: The View From Corporate Finance

EU TO FIGHT CROSS-BORDER FRAUD

A new office will address corruption across national boundaries.

European Union (EU) justice ministers have agreed to establish an independent public prosecutor's office to investigate and prosecute criminal cases affecting the EU budget, including corruption or fraud with EU funds and cross-border value-added tax (VAT) fraud. Twenty of the EU's 28 member states will work with the new office.

The Luxembourg-based prosecutor's office will have the ability to respond quickly across national borders, without the need for lengthy judicial cooperation proceedings. It will bring actions against criminals directly in front of national courts, streamlining investigation and information-sharing. The European Commission says cross-border fraud costs EU member states an estimated 50 billion euros ($57 billion) in VAT revenue annually.

Currently, only national authorities can investigate and prosecute EU fraud, and existing EU bodies do not have the authority to conduct criminal investigations. **– D. SALIERNO**

WOMEN LOSING GROUND

Fewer women were appointed to U.S. boards in 2016 in a setback for gender parity.

Female directors lost ground for the first time in seven years, according to Board Monitor: Board Diversity at an Impasse?, the latest annual study from executive search firm Heidrick & Struggles. Women accounted for 28 percent of new director appointments at Fortune 500 companies in 2016, down 2 percent from the previous year.

"It is disappointing to see that more progress wasn't achieved to move closer to gender parity in corporate boardrooms in 2016," says Bonnie Gwin, vice chairman and co-managing partner of

IMAGES: TOP, SASHKIN / SHUTTERSTOCK.COM; LEFT, ROBSONPHOTO / SHUTTERSTOCK.COM the company's global CEO & Board Practice.

Fortune 500 boards filled a record 421 seats in 2016. Of those new directors, almost 75 percent had previous board experience. Yet when companies place more value on a candidate's unique skills and experiences vs. board experience, women and people from other underrepresented groups gain greater representation in the boardroom, Gwin says. Women accounted for 37 percent of new board appointees who are serving on boards for the first time.

One industry where women made big gains is the technology sector, where board diversity has lagged behind other sectors. Women accounted for 40 percent of newly filled board seats, up 13 percent from 2015. Gwin notes board diversity at tech companies has increased following the Hewlett-Packard and Hewlett-Packard Enterprise split in 2015, when four women and two people of color were placed on each new board.

Hispanic director appointments rose sharply from 4 percent in 2015 to 6.4 percent in 2016. "This increase is due to more boards focusing on inclusion, and an effort to have companies' boardrooms better reflect their customer base and employee population," says Jeff Sanders, vice chairman and co-managing partner of Heidrick & Struggles' global CEO & Board Practice. **– S. STEFFEE**

GUARDING AGAINST RANSOMWARE

Internal audit can help scrutinize cybersecurity practices and plans, says **Soo-young Lee,** lead internal auditor at Songwon Group.

What should internal auditors ask to assess the organization's protections from ransomware attacks? Now is a time of unprecedented state-on-state ransomware attacks. To protect an organization from these attacks, internal auditors should question whether senior executives and the board support designing a holistic approach for people, process, and technology to make a defense strategy successful. Does IT security governance include the human factor in its corporate risk analysis and assessment? Is there a business continuity/disaster recovery cyber breach program that originated from a business impact analysis that includes vulnerability assessment and ethical hacking?

What is the most important deterrent to mitigate the risk of an attack? Employees are an organization's greatest asset, but also its greatest security risk. As new types of cyberattacks grow, organizations must do people "patching" – training employees on how to recognize, analyze, and respond to vulnerabilities. Those vulnerabilities include out-of-date operating systems and software, and suspicious emails and attachments. Also, IT should make sure antivirus programs are installed and that files are backed up daily somewhere not connected to the internet.

CULTURE OF RESILIENCE

New guidance offers keys to addressing organizational crises.

A new IIA report examines how internal auditors can help organizations progress from mere "crisis awareness" to a culture of "crisis resilience." Organizations that achieve this transformation can better resist, react to, and recover from major disruptive events, according to Global Perspectives and Insights: Crisis Resilience.

Responding to a crisis can involve much more than just restoring operations, the report notes, especially when lives are lost, customer data is compromised, or a CEO is humiliated. Internal auditors can expand their roles and step back to consider the big picture—the broad organizational objectives and corresponding risks. "They can help prepare their boards, executives, and employees for a crisis, provide assurance over readiness, and help instill a crisis-resilient culture," the report says.

Crisis Resilience also points to the role of internal audit in post-crisis activities, responding to lessons learned. Participating in this process provides an opportunity for auditors to move from a supportive to a front-seat role in the organization, the report concludes. **– D. SALIERNO**

PHOTO: RIGHT, OATAWA / SHUTTERSTOCK.COM

BY BRIAN AIKEN + DAVID CODERRE EDITED BY JAMES ROTH + WADE CASSELS

MORE THAN COMPLIANCE WITH "A"

Transforming a compliance program into a value-adding activity starts with internal audit.

It is difficult to argue that compliance audits are not an important internal audit product. Noncompliance with, for example, anti-money laundering legislation can have serious consequences. In one recent example, Deutsche Bank was fined $425 million by the New York State Department of Financial Services and $204 million by the U.K. Financial Conduct Authority for failing to conduct basic money laundering due diligence.

Despite the seriousness of noncompliance, many managers do not see compliance audits to be of value, possibly because they often look like this:

- Objective: Verify compliance with "A."
- Criterion: Client should do "A."
- Condition: Client is not doing "A."
- Recommendation: Do "A."

Auditors need to ensure that compliance audits provide real assurance to senior management and add value.

Do the Right Thing

Internal auditors can add value to compliance audits by doing the right audit and doing it correctly. Doing the right audit means examining why there is a compliance requirement in the first place. Typically, it's for legal, regulatory, operational, or ethical reasons. But behind "you must do 'A,'" there is a serious enough risk for management or regulatory/legal authorities to put in a compliance requirement. However, risk shifts quickly, and speed of change is a critical success factor of business. Risk morphs rapidly in a world where globalization and automation affect strategic and operational initiatives of global enterprises. Changing risks can affect not only the need for compliance controls but also their adequacy. In addition, while the compliance function monitors noncompliance, internal audit provides the independent assessment over risk as the third line of defense.

Internal audit provides assurance on the effectiveness of governance, risk management, and compliance, including the way in which the first and second lines of defense achieve risk management and control objectives. This assurance covers a broad range of objectives, including compliance with laws, regulations, policies, procedures, and contracts. But it should not be compliance simply for compliance sake. Internal audit should consider the overarching business objective and the controls that help mitigate risk to the achievement of the objective—even when examining compliance-related controls.

Deconstructing the top-level strategy into key objectives will identify the enterprise-level risks that threaten achieving those goals, the process-level control objectives that mitigate enterprise risks, and

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

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

process-level risks and controls. The compliance activities will likely be closely related to these process-level risks and controls, which should be assessed.

Start With the Objective

Virtually every company will have a set of policies and procedures that must be followed to protect it from lawsuits, prosecution, and reputational and other risks. These are the areas with compliance requirements and where audit performs compliance audits. For example, companies with manufacturing plants must comply with environmental regulations, and U.S. publically traded companies have to comply with the U.S. Sarbanes-Oxley Act of 2002 and other financial and legal rules and regulations.

Transforming a compliance audit into a value-adding activity starts with the audit objective. This defines what the audit seeks to accomplish and drives the scope, criteria, work plan, and final results. If the objective is simply to verify compliance with "A," then one will fall into the trap of concluding "You are not doing 'A'" and recommending "Do 'A.'" However, if the objective is "To verify the need for, existence of, and adequacy of compliance with 'A,'" it will be better positioned to address governance and risk management issues and compliance.

In this type of audit objective, one of the first steps would be to determine if the original risks and compliance requirements still exist. They may have been eliminated by a change in operations (e.g., the company is no longer making that product) or transferred to someone else (e.g., subcontracted out); the company is no longer using that manufacturing process; or business process re-engineering, changes in location, or retooling may have eliminated, transferred, or lessened the risk. In these cases, the value add might be the elimination of the requirement. No risk = no compliance requirement.

With a good understanding of the current level and sources of risk, the next step is to look at the requirement for, and the adequacy and effectiveness of, the mitigating control. This requires an understanding of the cause and source of the risk and the operation of the control. Is the control still required? Does it address the root cause? Are there better ways to mitigate the risk? By answering these questions, the audit may identify unnecessary, ineffective, or better controls, which may reduce the cost of compliance while improving risk mitigation. The next step would be to verify that the control activities are being performed (i.e., compliance). However, if one finds noncompliance, it is not sufficient to recommend "Do 'A.'" Audit recommendations should address the root cause, including determining why management is not complying. Was management aware of the requirement? Is management capable of complying? Are there compensating controls that have been implemented? Asking *why* (usually several times) is often sufficient to determine the cause of noncompliance.

Internal auditors also should determine the impact of noncompliance. Then instead of saying, "Do 'A,'" audit can provide a rationale and make a recommendation that assists management in complying.

Next, the audit should be done right. This means maximizing use of resources and analytics. Data analytics includes the application of analysis techniques to understand business processes; identify and assess risks; test controls; assess efficiency and effectiveness; and prevent, detect, and investigate fraud. Data analytics techniques can assist organizations in focusing their risk responses in the areas in which there is a higher risk—including compliance risk.

Existing levels of risk can be assessed and trends identified to determine whether the risk is increasing or decreasing. For example, environmental compliance could examine spills (number and quantity), clean-up costs, and lawsuits (quantity and value); while production compliance could examine material, personnel, maintenance, and operational costs. By examining measures over several months or years, trends can be produced to assess the effectiveness of mitigation efforts and identify emerging risks.

The effectiveness of controls also can be tested with analytics. For example, environmental compliance can examine the control over the purchasing of hazardous materials—ensuring that the purchase quantities match requirements—thereby avoiding environmental compliance issues around disposal. Compliance with hiring practices could review staffing methods and staffing rates (by gender, race, etc.) to ensure procedures are being followed and address employment equity requirements before they become noncompliance issues.

Remove the Stigma

Sometimes compliance with a poor control can increase risk and dysfunctional behavior, and cultural issues can make enterprisewide compliance difficult for global companies and increase risk. Doing the right compliance audit—not simply "did we do 'A?'"—and doing it effectively can result in significant value to the organization and remove the "gotcha" stigma of compliance audits. However, it requires auditors to re-look at the compliance-related risk and controls and use analytics. By doing so, it will add value and provide assurance to senior management about compliance-related risks. Ia

BRIAN AIKEN, CIA, CFE, *is the former assistant comptroller general of Canada in Ottawa, Ontario.*
DAVID CODERRE, ACDA, *is president of CAATS in Ottawa, Ontario.*

BY KEN GUO + WEI JIANG EDITED BY STEVE MAR

STOP CLICKING, START CODING

SQL queries can enable internal auditors to uncover greater insights from organizational data.

As data grows in volume and complexity, the effective use of it is critical for making better, faster, and more informed decisions. Organizations increasingly are seeking internal auditors who can analyze data and generate insights that bring new value to the business.

While internal auditors typically perform data analysis using specialized audit software packages or a general spreadsheet application, there is a growing need for auditors to develop technical skills beyond those tools. For example, Fortune 500 firms such as Google and Verizon have made proficiency in structured query language (SQL) part of their job requirements for hiring internal auditors.

SQL is a special-purpose programming language designed for managing data held in database management systems that support widely used enterprise resource planning systems. Designing SQL procedures for transforming data into useful information requires a good understanding of data structure and the logic of how a system works. Such understanding is particularly important for internal auditors when they work with large volumes of data in today's complex business environment. From the learning perspective, logical thinking and reasoning inherent in the SQL coding process helps internal auditors develop the critical thinking and problem-solving skills desired by the profession.

Moreover, SQL-based analysis has gained increasing importance with the advent of big data. SQL tools enable fast access to relational databases that store vast amounts of data, offer flexibility in developing ad hoc queries on an as-needed basis, and can be tailored to the specific needs of auditing. Furthermore, because SQL is an international standard, internal auditors are not constrained to using a specific software tool.

Asking Questions of Data

Internal auditors can write and refine SQL codes in a relational database to arrive at incrementally better solutions until the desired outcome is achieved. Consider the example of an Employees table that contains data such as employee ID, first name, last name, birth date, and hire date. Auditors can ask many interesting questions about this data, such as whether the company has complied with all employment regulations. In the context of The Committee of Sponsoring Organizations of the Treadway Commission's *Enterprise Risk Management–Integrated Framework*, this inquiry addresses the company's conformance with its compliance objectives.

To check compliance with child labor laws, internal auditors can query the data to determine whether

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

TO COMMENT on this article, EMAIL the authors at ken.guo@theiia.org

any employees were underage at the time of their hiring. For example, the minimum age for employment in the U.S. is 14; and there are specific requirements for the age group between 14 and 18. Auditors can begin answering this question using this code:

```
SELECT EmployeeID, FirstName, LastName,
    (HireDate-BirthDate)/365
    FROM Employees;
```

The SELECT statement in the code retrieves all of the values in the EmployeeID, FirstName, and LastName columns, and calculates the age of the employee at the time of hiring as the difference between the HireDate and BirthDate divided by 365 days. The FROM clause specifies the tables from which the data are selected.

The query returns a total of 11 employees. Of these employees, the results identify four questionable employees: two are under 18 and the other two have no age information. At first glance, the design of the query seems to answer the question, but this solution only works well for small organizations. Imagine a large company that has thousands of employees. In such a situation, auditors would have to sift through a long list of employees to identify those with age problems. An additional issue is that the system-generated title of the column for the age data, "Expr1003," is not descriptive, and the data, itself, has 10 decimal places. To address these drawbacks, internal auditors can improve the SQL statement:

```
SELECT
    EmployeeID, FirstName, LastName
    ROUND((HireDate-BirthDate)/365, 1)
    AS AgeAtHire
FROM Employees
WHERE (HireDate-BirthDate)/365 < 18;
```

This revision aims to filter out unnecessary data and improve the readability of the report. Adding the WHERE clause restricts the result to employees under age 18. The ROUND function rounds the age number off to one decimal place. The heading of the column containing the age data is also renamed to AgeAtHire. The query result now contains only two suspicious employees who were under 18 at the time of their hiring.

However, there is something missing from the report. The first query uncovered two additional suspicious employees without any age information. Further examination of the Employees table reveals that birth and hiring dates are not available for these two employees. While only a conjecture, these two individuals may have been "ghost employees" as the result of payroll frauds. Internal auditors should include these two suspicious employees in the report, as well.

To find this information, internal auditors can amend the SQL query:

```
SELECT
    EmployeeID, FirstName, LastName
    ROUND((HireDate-BirthDate)/365, 1)
    AS AgeAtHire
FROM Employees
WHERE (HireDate-BirthDate)/365 < 18
OR (HireDate-BirthDate) IS NULL;
```

In this solution, auditors add another condition "(HireDate-BirthDate) IS NULL" in the WHERE clause with the OR operator. The OR operator performs a logical comparison and specifies that an employee should be included in the report if either of the two conditions is met: age at the time of hiring is less than 18, or age data for this employee is NULL (i.e., left blank). Now the report shows all four suspicious employees.

This is not the end of the data analysis, however. Based on this result, internal auditors would need to investigate further to determine why the age information is missing for two employees and how the two underage employees were hired in the first place.

SQL and other audit software can form a powerful set of analytical tools.

Powerful Analytical Tools

The underage employee example demonstrates how SQL can be a useful database tool for solving audit-related problems. However, it has only scratched the surface of the capabilities of SQL-based data analysis. Indeed, SQL and other audit software can form a powerful set of analytical tools for internal auditors, particularly in the context of ever-growing volumes of data available for business use.

KEN GUO, PHD, CPA/CMA (CANADA), *is an assistant professor at California State University, Fullerton.*

WEI JIANG, PHD, *is a professor of accounting at California State University, Fullerton.*

BY KEVIN SHEN EDITED BY CHARLIE WRIGHT

INTERNAL AUDIT NEEDS RISK MANAGEMENT, TOO

Managing its own risks can improve the audit function's performance and demonstrate that it practices what it preaches.

Part of an internal audit department's mission is to ensure that the organization has effective governance and management around its risks. But what about internal audit, itself?

Audit departments face similar risks to other corporate functions. If internal auditors cannot manage their own risks appropriately, it is hard for them to educate others about the need to manage their risks effectively. Auditors should practice what they preach.

Internal audit's risk management program should result in risks being managed like in any other competent risk management program. The audit function needs to identify all relevant risks; perform risk assessments; set its risk appetite; mitigate, manage, avoid, transfer, or accept the risks; and continuously monitor the risks.

Risk in the context of internal audit can be defined as an uncertain event or condition that, if it occurs, has an effect on at least one internal audit objective. As such, internal audit should start by examining its mission and objectives, which are typically defined in the internal audit charter approved by the organization's board of directors or audit committee. By understanding internal audit's key objectives, auditors can then identify the risks that can prevent them from achieving those objectives.

Strategic Risk

One of the most significant risks is strategic risk. For internal audit, one risk is whether the department is strategically positioned within the organization to achieve its objectives. Other considerations include whether the department has the authority, independence, and objectivity to provide assurance and help the organization improve its risk management; whether it is focused on assurance or financial recoveries; and whether the audit team has the right personnel.

Strategic risk also could arise when audit strategy does not align with the organization's overall strategy. For example, this can happen in an organization that is planning to expand into emerging markets when internal audit is not equipped to cover anti-bribery and foreign corruption risks associated with the expansion. Every organization is different, but the chief audit executive (CAE) can generally manage this risk by refining the internal audit charter; interacting with the board, senior management, and other stakeholders; and ensuring risk assessments and audit plans are up to date.

Reputation Risk

Credibility is the most important asset of any audit function. Reputation risk is the potential that negative publicity regarding internal audit's practices will cause a decline in trust in the

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

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

department. Misconceptions about internal audit can damage its ability to achieve its objectives. Also, reputation risks can arise from operational or compliance risk.

This risk can be managed by maintaining timely and efficient communications among stakeholders, reinforcing ethics, creating awareness at all staff levels, developing a comprehensive audit methodology, focusing on risk and built-in controls, responding promptly and accurately to stakeholders, and establishing a quick response team in the event there is a significant action that may trigger a negative impact on the function. A strategically positioned internal audit function also may be better prepared to defend its own reputation.

Compliance Risk

Compliance risk is becoming important for internal auditors, particularly in highly regulated industries such as large banks. For example, the U.S. Office of the Comptroller of the Currency created Heightened Standards that includes guidelines about the roles and responsibilities of internal audit. The Federal Reserve Bank has issued a Supplemental Policy Statement on the Internal Audit Function and its Outsourcing.

As audit departments get deeper into data analytics, compliance with consumer data and cross-border privacy laws could become a concern. The key to managing the risk is to thoroughly evaluate the laws and regulations and address them through internal audit's own policies and procedures as well as ensuring the ability to demonstrate compliance with the rules. Internal reviews performed by an independent quality assurance team can help identify potential issues and prevent noncompliance incidents.

One of the most relevant risk categories to internal audit is operational risk.

Operational Risk

Apart from the previous risks, the category most relevant to internal audit's day-to-day activities is operational risk, which consists of risks that arise from deficiencies in people, process, or technology. Like other departments, internal audit has specific operational goals such as completing the annual audit plan, validating audit-identified issues, maintaining costs within a defined budget, and developing a skilled workforce.

A systemic approach should be taken to manage the operational risks, including creating operational risk appetite, developing key performance and risk indicators, monitoring, and taking actions to mitigate the risks. For example, to ensure timely completion of the audit plan, it may be helpful to closely monitor audit start, fieldwork completion, and report dates. A dashboard stratified by teams may help manage each team's execution risks. A graph about quality assurance review results by team also may enable the CAE to identify teams that have issues with executing audits and provide training to remedy the risk.

Once identified and defined, internal audit should establish thresholds to monitor and mitigate the risks. Color codes could highlight areas of focus. For example, if more than 20 percent of the audits in progress are delayed more than 30 days, a red status may indicate the risks to timely completion of the audit plan. If one team's turnover ratio is more than 20 percent, it may be time to highlight the risk as red for action.

The thresholds are dependent on the CAE's risk appetite, but they also should consider input from key stakeholders. For example, the CAE may want to specify that no more than 5 percent of the audit plan may be carried over into the next calendar year. If that target appears to be at risk, then the CAE should take action to mitigate risks. For example, if turnover around a certain time of the year is elevated, a prenegotiated cosourcing arrangement may help mitigate the risk of not completing the audit plan.

Furthermore, internal audit should apply the organization's enterprise risk management polices where relevant, at least in principle. For example, when operational incidents such as near misses—incidents that almost happened—occur in internal audit activities, internal audit should file internal incident reports, analyze root causes, and prevent similar events in the future.

Better Risk Assurance

In addition to risk indicators, thresholds, and incident tracking, other useful tools exist. For example, internal audit can use a risk control matrix to perform a risk control self-assessment that evaluates the adequacy of internal controls in place within the department. By creating a library of risks and corresponding controls and self-evaluating periodically, internal audit departments can have better assurance about their own risks.

A holistic approach to managing internal audit's strategic, reputation, compliance, operational, and other risks can bring more consistent performance. Moreover, it can better position the department to help the organization improve its risk management process. Ia

KEVIN SHEN, CFA, CPA, *is vice president, Internal Audit, at HSBC USA in New York.*

Fraud Findings

BY JAMIE HOELSCHER EDITED BY BRYANT RICHARDS

THE CASHIER CASH THIEF

Mounting family pressures and opportunity cause a trusted warranty clerk to pocket payments from customers.

James Audette was a cashier and warranty clerk for a car service repair shop. His main responsibilities were submitting warranty claims and accepting payments from customers in the form of cash, check, or credit card. Audette quickly learned the ins and outs of handling customer payments and discovered that no receipt of payment was generated for service tickets that were covered by the customer's extended warranty. Instead, those tickets were closed to accounts receivable (warranty companies). In addition to submitting warranty claims and accepting customer payments, Audette also was responsible for creating the journal entries and posting to the general ledger. On a monthly basis, the controller would review the journal entries and general ledger account to ensure everything balanced.

It was known that money was tight for Audette and his family. In addition, his son struggled with drug addiction, and he and his wife were continually trying to help him. On several occasions, Audette had taken out personal loans from the company, but he always repaid them on time. Audette rarely missed work and was always eager to work overtime, often staying late and volunteering to work weekends to satisfy his debts.

Audette was a loyal employee. One day, however, mounting family pressures led Audette to pocket a customer's cash payment and record the ticket as warranty work. By classifying the ticket this way and establishing the receivable, the customer would not be billed at a later date and the customer's account balance would be accurate. Audette began to routinely close customer tickets as warranty work and pocket the money when customers paid in cash. To conceal the fraud, he would clean the schedules each month by crediting accounts receivable and debiting labor (a cost of sale account), but would provide no journal entries for these "write offs," thus making the general ledger balance appear to reconcile with the journal entries provided to the controller for his review and reducing the physical audit trail. This activity continued for several months, with the thefts becoming larger over time until Audette was promoted to a new department within the company.

Lauren Simpson was hired to replace Audette as warranty clerk and cashier, but Audette maintained his old duties to conceal his previous thefts and continue to write off the receivables he created to avoid further detection. Simpson complained about Audette's continued involvement in his old role so the controller restricted his access login and alerted Russell Perez,

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

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

LESSONS LEARNED

- » Internal auditors must emphasize the importance of segregation of duties and closely monitor any possible exceptions. In this example, having one individual responsible for the collection of cash receipts and the subsequent recording (journalizing and posting) leaves an organization susceptible to the theft of cash.
- » Internal auditors must not assume that accounts that are in balance preclude the possibility of errors, omissions, or thefts.
- » Access controls should be immediately updated following an employee's promotion, termination, or changing of job responsibilities. Internal audit should be at the forefront of ensuring policies and procedures are in place to limit logical access controls and that such policies are being enforced, including annual reviews.
- » Trend analysis would allow an organization to detect such fraud more timely, as the percentage of cash payments drastically increased, while the percentage of warranty service drastically decreased, over the period. Even basic analytics can aid in the foundation of an effective analytics program, while also limiting the perceived opportunity for fraud.
- » An audit of a small sample of warranty claims would have revealed those tickets had previously been paid in cash.
- » Routine audits are vital for all cash processes. Even the knowledge of a potential audit can help mitigate the perceived opportunity to engage in fraudulent activities. Routine execution of the audit enhances the ability to detect existing abnormalities quicker, thus mitigating the impact of any existing fraud.
- » Mandatory vacations and rotation of duties could have prevented the fraud from happening, or brought it to light sooner. Internal audit should be at the forefront of ensuring policies and procedures are in place that require mandatory vacations and that those policies and procedures are being enforced. Basic queries can easily identify employees not abiding by this policy, creating another simple, yet effective foundation to any data analytics/fraud detection program.
- » The most well-liked and loyal employees are capable of fraud, and often have the most opportunity to misappropriate assets. Internal auditors must continually exhibit objectivity and maintain professional skepticism through all aspects of their job.

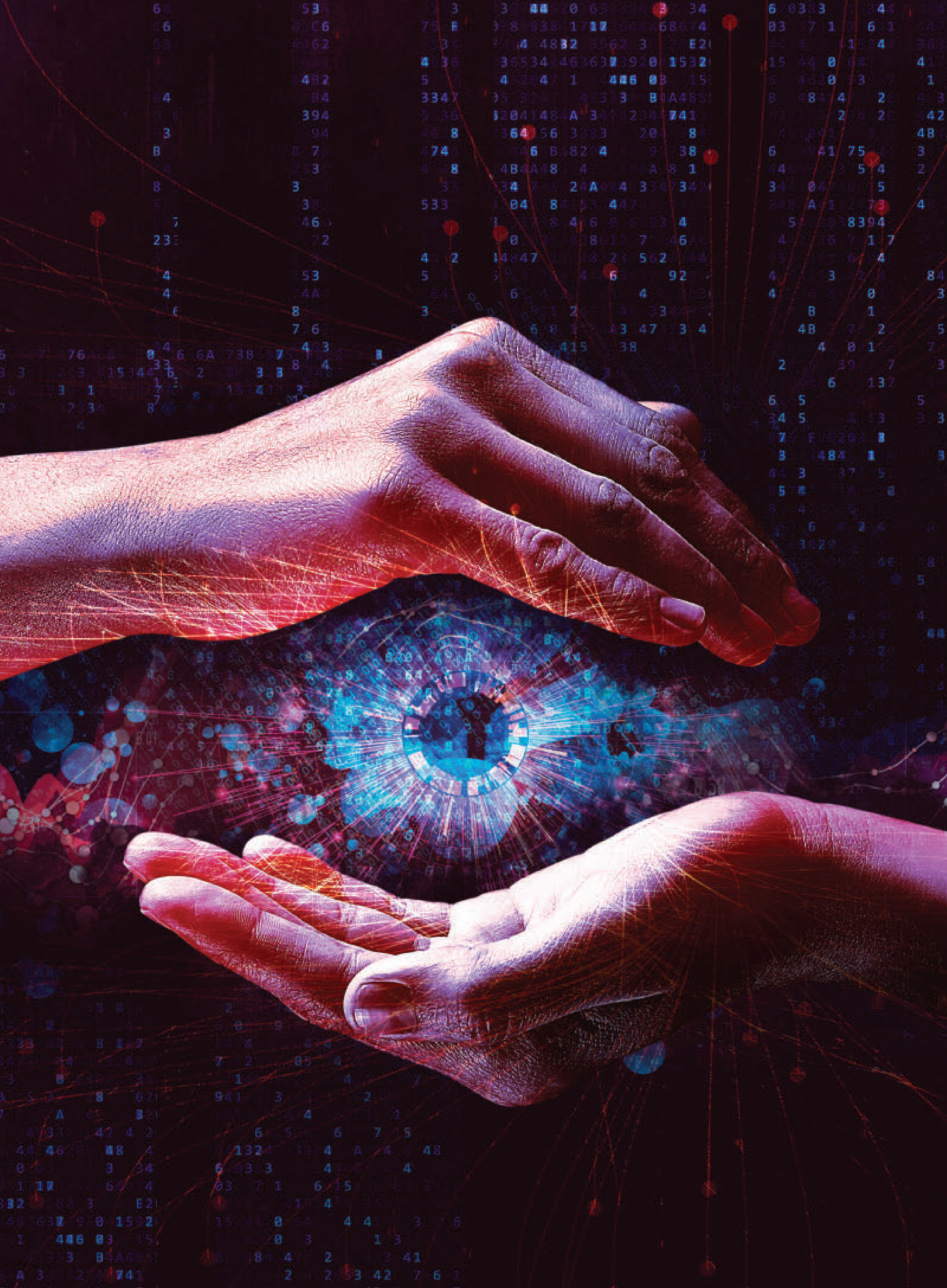
the company's internal auditor. Perez requested that Simpson run the accounts receivable schedules older than 90 days that were not paid. She pulled the tickets, which were stamped "paid in cash." To confirm, the general manager called the customers on those tickets and inquired about their service and ease of use of the "new credit card reader." Each customer whose ticket was in question promptly responded by saying he or she had paid in cash and had not used the new credit card reader, thus confirming the theft of cash payments. Perez then examined the entire population of tickets closed out by Audette, going back several months, and uncovered additional tickets closed as warranty work that were actually paid in cash and later written off. Perez met with company management to discuss the likely magnitude and nature of the fraud.

Employees were alerted of the potential fraud and asked to come forward with information. Ironically, Audette came forward with his suspicions of a fellow employee. Consistent with company policy, employees were told they were going to be subject to a lie detector test. Audette never returned to work. When the company contacted him, he denied any knowledge of the fraud and stated that he did not want to work for a company that did not trust him and would accuse him of such actions.

Internal auditors worked closely with management following the detection of the fraud, performing a complete review of internal controls in the cash receipts function and other functions, as well. The comprehensive review served to not only decrease the perceived opportunity to engage in fraudulent activities among other employees, but also to detect any other abnormalities existing in other areas of the business. Internal auditors also emphasized the importance of more routine reviews of processes and key controls.

Audette's employer did not want to consume company resources and effort with litigation so he was never prosecuted. The fraud totaled $5,000 but was likely much larger, as the audit only went back a few months to the beginning of the fiscal year and further investigation did not ensue. Ia

JAMIE HOELSCHER, PHD, CIA, CFE, *is an assistant professor of accounting at Southern Illinois University–Edwardsville.*



Arthur Piper

Illustration by Sean Yates

In Safe Hands

Organizations must grapple with a host of issues when determining how to best protect their data and manage the way it's used.

"There is no business today that is not driven by data," Dominique Vincenti, vice president, Internal Audit and Financial Controls, at Nordstrom in Seattle, says. "The continuous high-speed evolution of technology is the No. 1 challenge for businesses and internal auditors today. There is not an hour you can rest."

Vincenti says that businesses need to fundamentally reassess what data means to the success of their organizations going forward. Not only must they be able to successfully protect their data from external threats, but a new law is sparking a trend that will require many to have much more detailed control over what data can be held and how it can be used—the General Data Protection Regulation (GDPR) that goes into effect in Europe in spring 2018. Add to that data processing developments in data analytics, robotics, and artificial intelligence, and organizations that are unable to leverage their most business-critical asset effectively are in danger of being left behind, or worse.

"There needs to be a huge wake-up call," Vincenti says. "Businesses need a clear answer to the question, what does data mean to the success of our company both today and tomorrow?"

The conjunction of GDPR and advanced data processing technologies is pushing organizations into new ground. For businesses operating in Europe, or any business using or holding data on European citizens, for example, the tougher new data laws will substantially alter the way that organizations need to seek consent and keep data records (see "Main Provisions of GDPR" on page 29). "GDPR is a more

FOR MORE INFORMATION on protecting organizational data, see the IIA Practice Guide: Auditing Privacy Risks, 2nd Edition." http://bit.ly/2tnlf5i

stringent regime than those it replaces, and has a low risk appetite built into it," Vincenti says. "Since Europe tends to lead the way in legislation, it would be wise for U.S. businesses that are not affected today to at least consider how they might meet those requirements in the future."

GDPR's heavy fines have caught the media's attention—the maximum is 4 percent of the organization's global revenues. For example, telecom and broadband provider TalkTalk's 2016 fine of £400,000 from the U.K.'s Information Commissioner's Office for security failings that allowed hackers to access customer data could have rocketed to £59 million under GDPR.

Yet having the right controls over how data is used and retained will present a challenge. For example, businesses will no longer be able to request a blanket consent to use data collected from individuals in any way they choose. Consent will need to be obtained for a specific and detailed use—otherwise fresh consent will be required. This provision is diametrically opposed to how data can be leveraged by artificial intelligence and data analytics programs. Such programs are best used to find new patterns in data and novel applications of information to improve the business' products and services. Without free license to experiment with customer data on the business' servers, it may not be possible to achieve the full potential these technologies promise.

For internal auditors, these pressures could mean going back to the drawing board on the controls needed to strike the right balance between delivering value to stakeholders from these new technological possibilities and protecting the enhanced rights many customers will enjoy under GDPR. A compliance-based approach may no longer be feasible because it is unlikely to capture the nuances needed

"GDPR is a more stringent regime than those it replaces, and has a low risk appetite built into it."

Dominique Vincenti

to deal with this ethically sensitive area. In fact, many are arguing that successfully handling the new data landscape will require auditors to develop ethical principles and soft skills that have been undervalued in this area.

"Respecting someone's privacy rights is actually a soft skill and needs a soft approach."

Henry Chang

THE CHALLENGE OF CONSENT

"If you don't know what you are going to discover from a big data project, how can you possibly explain to the data subject how you will use it and get consent?" Henry Chang, an adjunct associate professor at the Department of Law at the University of Hong Kong, says. Chang is one of several academics and business organizations arguing that new regulations such as GDPR coupled with new technologies require a paradigm shift when it comes to personal data use and protection. Chang and Vincenti agree, for example, that organizations pursuing a compliance-based approach to data privacy and protection are going to run into a brick wall when trying to leverage their data innovatively.

"When you look at a compliance-based approach, you have to decide where the pass-mark is legally," he says. "That tends to cause businesses to aim low and achieve low, and businesses can spend a lot of time on trivial areas because they think they need to comply in every part of their business equally, rather than where they are most at risk."

He says what is required instead is a more holistic, accountable approach that has privacy controls engineered into business processes, which themselves are underpinned by ethical principles. While there is no magic solution, he urges organizations to try a cocktail of approaches to see what works best. For example, he says that data privacy is built on the notion that one has respect for the individual's right to have a say over how that information is used. Compliance cannot address how those rights might change over time if the systems used to comply

Only 9% of U.S. companies responding to a recent Experian survey report that they are ready to comply with the GDPR; 59% do not know what they need to do to comply.

MAIN PROVISIONS OF GDPR

Article 5 of the General Data Protection Regulation requires that personal data shall be:

(a) Processed lawfully, fairly, and in a transparent manner in relation to individuals.

(b) Collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

(c) Adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.

(d) Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

(e) Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific, or historical research purposes, or statistical purposes subject to implementation of the appropriate technical and organizational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.

(f) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organizational measures.

Article 5(2) requires that "the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

Source: U.K. Information Commissioner's Office

with regulations do not have some elasticity built into them.

"Respecting someone's privacy rights is actually a soft skill and needs a soft approach," he says. "Putting in an ethical boundary as an extra element into your compliance processes could help deal with shifts in the way that personal data can be analyzed and used."

In practice, that could mean that if a company is using automated processes, some part of those systems could include a right for decisions to be made by a human. Or where mistakes are made with the use of data, there is a human at the end of the process and effective redress mechanisms in place.

"The head of audit's role could be to bring these debates to the attention of the board," he says. "You obviously cannot prescribe a set of ethics to the board, but you can ensure that the board has the opportunity to think ethically about personal data."

A BALANCING ACT

While obtaining consent for the use of data may seem reasonable, what happens if the potential uses are beyond the understanding of the individuals involved? According to the Information Accountability Foundation (IAF), a global research nonprofit, there is a growing agreement that consent is not fully effective in governing such data and use. Many national laws include limited exemptions for processing when consent is unavailable, while others, notably European law, provide legal justification based on the legitimate interest of an organization when it is not overridden by the interest of the individuals. But such exemptions tend to be limited, unclear, or outdated, and those legitimate interests require a balancing procedure that has yet to be developed.

"Companies are meant to balance the legitimate interests of individuals, organizations, and shareholders," Martin Abrams, executive director of IAF in Plano, Texas, says. "That means not only looking at the potential negative impacts on individuals, but on stakeholders, too, if you do not process that data."

For example, Abrams says, next-generation clinical research by pharmaceutical companies could draw data from multiple devices—smartphones and watches, genomics, location-sensitive information, and clicks on webpages—into the data pool in a way that could be difficult to describe to people who are asked to consent

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

because it is unclear how the various interests at play can be balanced. If some of that data is European, a difficult problem could become intractable. “It’s not clear how one could do data analytics under GDPR,” he says.

The IAF has been working with the Canadian government to test an ethical assessment framework it has created to help organizations develop accountability processes that go beyond the consent model. It aims to provide a common framework for developing systems of accountability and for ranking the importance of potentially conflicting interests for each project.

Internal auditors, he says, should be asking their boards to think about how the business is balancing the various interests at stake in its use of data. How those decisions and processes are documented and assessed, and whether the business has the right skill sets to implement such an approach, could all be the topic of audit assignments.

TRANSPARENCY AND COMMUNICATION

One approach to addressing data concerns is for businesses to become as transparent as possible about their aims and objectives and how those interests are balanced. “It is very important for the business to tell a clear story about what its intentions are, how it is going to use the data, and how that will be for the betterment of society,” says Lisa Lee, vice president, Audit, at Google in Mountain View, Calif.

She says that innovation requires research and having too many rules around how data can be used could stifle developments that could benefit the community. Too many checklist-style controls are unlikely to keep pace with the speed at which technology is developing. That is why Lee says that companies need to engage people in dialogue about their ethics and articulate the benefits to society they are attempting to deliver.

“We work in a very dynamic environment and need to keep an open mind when we are thinking about controls. ...”

Lisa Lee

Not everyone will align with a story. Lee says that people often have different tolerances to technology notifications, for example, and what one person would find useful, another might find intrusive. Business units need to have thought through those issues and communicate how they approach such risks and what the controls are for doing so. She says Google sets the tone for its values from the top of the company and those values inform its protocols, how it operates, and how it attempts to manage risks.

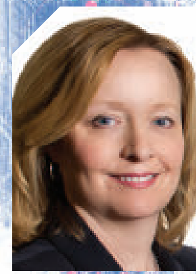
This approach impacts how internal audit works. “Internal audit has to have a very in-depth grasp of the business,” she says. Unlike organizations that tend to pool auditors into one team, Google has some dedicated audit teams attached to particular areas—such as data security and privacy—where a deep understanding of the systems is necessary. In addition, auditors focus on what the business objectives of the product or service are during an audit and spend time listening to how the business is attempting to approach risk and control.

“We work in a very dynamic environment and need to keep an open mind when we are thinking about controls and their impact or effectiveness,” she says.

GRASPING THE DATA

Few companies are as advanced in their handling of data as Google. One of the most common problems organizations face is that they do not know where their data comes from, how it is used, and in many cases, what data they hold. Mark Brown, vice president of Software Solutions and Services at the risk management software company Sword Active Risk in Maidenhead, U.K., recently estimated that only about 1 percent of businesses could pull in and analyze internal and external data in a meaningful way.

“One of the biggest challenges when it comes to data is knowing



“One of the biggest challenges when it comes to data is knowing what you have.”

Shannon Urban

Approximately **two-thirds** of U.S. businesses say that the **GDPR** will require them to rethink their strategy in Europe, according to a report from research and consulting firm Ovum Ltd.

what you have," says Shannon Urban, executive director with EY in Boston and 2017–2018 chairman of The IIA's North American Board. "As businesses have grown through expansion and acquisition, they have continued to accumulate data with no formal inventory." In addition, is it easy for data to move around the organization via enterprise resource planning systems, email, and mobile devices, making it possible for it to be used in unintended ways.

"If you don't have an identification and classification process that can identify what is sensitive, then using it effectively, never mind ethically, is going to be impossible," she says. "The models internal auditors use can sometimes be a bit upside down—we make sure the data is accurate and complete, but spend less time on whether it is appropriately sourced and accessed. That could mean rethinking our audit plan and checking that we properly source the competencies to deal with these issues," she adds.

Urban says it is important not to get overwhelmed. If auditors find their organization's data is unstructured, she advises them to take a risk-based approach and start with the information that is most critical to the business, including intellectual property, employee, and customer data. "It is completely within internal audit's purview to connect the dots and think about data across business lines," she says.

CENTER OF EXCELLENCE

Internal audit can take a lead in bringing their organization up to speed with these new challenges about the nature of data and technological innovations in data processing. "Internal auditors need to be well-versed in these developments and be able to educate management through our audits," Nordstrom's Vincenti says. She says internal auditors should make their function a center of excellence not only in both data protection and privacy practices but also in data governance and rapidly evolving enterprise information management approaches and capabilities. "Internal audit can be a role model. Let's show the business how we are using data in innovative and ethical ways," she says. Ia

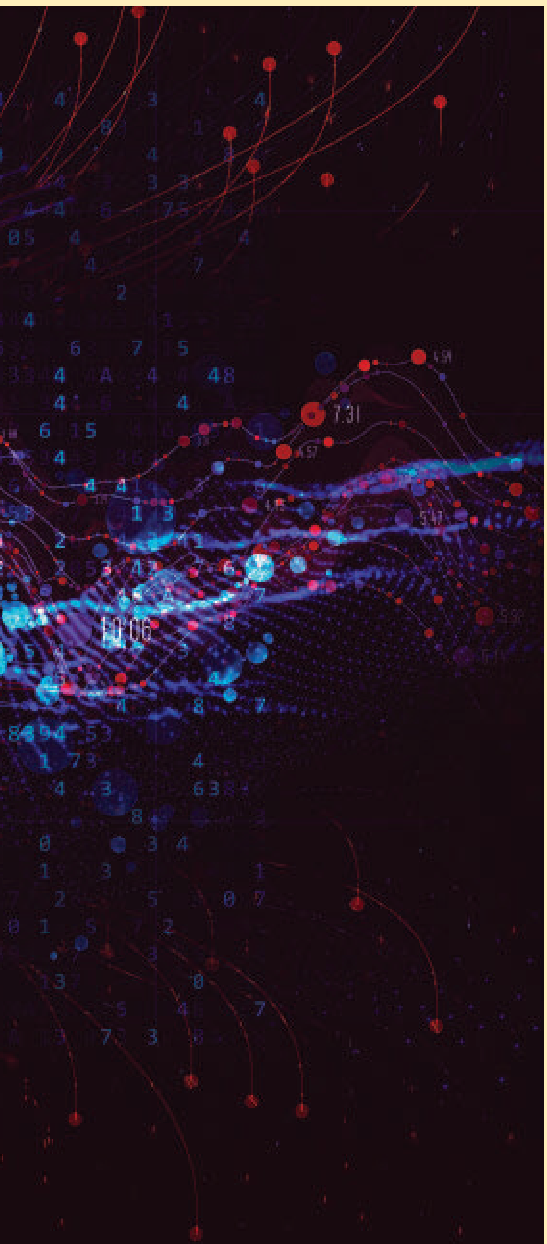
ARTHUR PIPER *is a U.K.-based writer who specializes in corporate governance, internal audit, risk management, and technology.*

As technology becomes more integrated with business processes, auditors must raise their IT skills.

Great tech Expectations

Russell A. Jackson

Illustration by Sean Yates



Internal auditors have always needed basic IT skills, a working knowledge of common audit tools, and a functional understanding of their organizations' data processes and infrastructure. What has changed in recent years as technology advances, and what will change in the future as it continues to, is what constitutes "basic," "working knowledge," "common," and "functional."

Some internal audit leaders note that new hires generally have better IT skills on day one than many veterans possess. That's not surprising for a generation of practitioners raised on smartphones and entering the workforce in an age of wearable devices. These auditors want to use their IT skills on the job as often as possible, blurring the line between internal auditors and IT audit specialists.

But that fuzzy border is also the product of a shortage of people with exceptional IT skills who want to be internal auditors. Those IT specialists will be as much in demand in the future as they are now. For chief audit executives (CAEs), that means balancing the need for core audit skills with the mandate for IT expertise in areas that may not have existed just a few years ago.

THE BASICS

"It's hard to succeed in any audit role today without some basic technology skills," says Steve Sanders, vice president of internal audit at Computer Services Inc. in Paducah, Ky. That includes both hard and soft skills — the latter an area in which some of the cleverest IT hands aren't adept. The basic software skills, like word processing, spreadsheets, and calendar and scheduling functions, should be assumed, Sanders adds. And he says, "auditors who have other software experience, such as electronic workpapers and, especially, data analytics, will have an advantage over those who do not have it."

Moreover, experience with audit-specific software is always a plus, "but these applications can be learned on the job," notes Jennifer Goschke, vice president and CAE at Office Depot in Boca Raton, Fla. That also helps keep practitioners from becoming proficient in the wrong kind of IT, developing skills on a particular brand of software at a previous job, for example, that don't translate to what's used by the auditor's current employer.

Outside the internal audit department, auditors need a big picture view of the IT landscape. In Goschke's department, "having a high-level understanding of the company's overall IT infrastructure and applications used" is foundational. In addition, every internal auditor should be familiar with IT general controls and the broad risks they were designed to help mitigate, she says. It's also important to understand key data security concepts—the principle of least privilege, passwords, and authentication—although it may not be necessary to have detailed knowledge of the IT used in specific departments.

In addition, auditors should understand how data is integrated into business processes, says Kathy Robinson, CAE at ADP in Roseland, N.J. "Regardless of the auditor's focus, he or she certainly needs to know where data resides, how it flows, and how it is accessed," she explains. That knowledge comes from the training she provides, as does a working understanding of data analytics. Some of ADP's auditors have become subject matter experts in data mining, in fact, and all of them can develop specifications for a project.

Controls are a good starting place for ensuring the audit staff is adequately versed in IT. Although new auditors are starting out with better IT skills, "they still need an understanding of controls," Sanders points out, "and new hires do not necessarily have a better understanding of controls than experienced auditors possessed 10 years ago."

Often, the auditors who excel in technical areas don't excel in soft skills, such as communications, empathy, and relationship building. New hires' tech-savvy "doesn't necessarily translate into their understanding of IT risk," Goschke comments. That lack of understanding can impede their ability to interact effectively with engagement clients. "Younger auditors need the more mature practitioners to help them communicate the risks and other issues to upper management," she says. Younger team members, she adds, "tend to favor short, digital conversations." Sanders notes that a well-qualified candidate should understand

"In-depth IT audits need auditors who understand those areas well enough to speak the language of the folks doing the job."

Steve Sanders

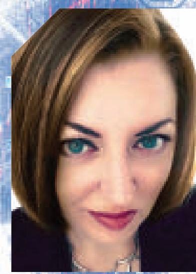
what was tested and "how to convey that to other stakeholders."

SPECIALISTS STILL IN DEMAND

Even if the rising level of IT expertise that internal auditors generally bring to the table isn't necessarily sufficient to get the job done without additional soft skills, the new auditors' computer skills are definitely changing the distinctions between internal auditors and IT auditors. "We're not asking our auditors to be IT technical specialists," Robinson explains, "and we're not asking people to do what they're not technically trained to do, because we have auditors with specific skills. But we are asking people to have a good understanding of data flow, controls, and governance."

Because IT audit personnel can be difficult to find, afford, and retain, it may be more cost-effective to cross-train the existing audit staff on IT risks than to hire a group of IT auditors. But even then, Goschke emphasizes, "it's important to have IT subject matter experts on your team to provide the technical chops to be able to go head to head with IT."

That's one reason why IT audit specialists still are in high demand. "An auditor with some technology background and a good understanding of controls might be able to do a basic IT audit," Sanders explains, "but in-depth IT audits need auditors who understand those areas well enough to speak the language of the folks doing the job." He notes that he's aware of several audit departments that use all auditors for IT audits. "The quality of work suffers just as it would if you assigned trained IT auditors to conduct financial audits," he says. "They might be able to do it, but they'll miss key things experienced financial auditors wouldn't miss. I've met some auditors who really don't have a good understanding of what they're looking at. They're not providing the value they need to provide."



"Younger auditors need the more mature practitioners to help them communicate the risks and other issues to upper management."

Jennifer Goschke

38% of CAEs rate general IT skills among their most desired qualifications for internal audit jobs, and 31% seek data analytics skills, according to The IIA's Top 7 Skills CAEs Want report.

CAES FACE HIGHER IT BAR

Nobody thinks every CAE should excel at IT, but expectations are pretty high. The bottom line: CAEs need to conceptually understand IT risk and hold their own in a conversation about strategic IT questions, even if they don't understand "the OSI model" or "Active Directory administration"—except, perhaps, in technology-focused companies. Citigroup's Mark Carawan puts it this way: "The CAE is responsible for ensuring the internal audit function stays relevant and nimbly adjusts to emerging risks and solutions. But the CAE is not responsible for being the fount of all knowledge."

CAEs should know the IT risks the organization faces—privacy, security, data management, and maintenance—and how management is or isn't addressing them. Although they needn't be able to answer every IT question that comes up in day-to-day engagements, CAEs should be able to ask good questions. They should augment their staff with a strong IT audit manager or director. Says ADP's Kathy Robinson: "There's nothing wrong with 'old school' CAEs, as long as their thought processes are ahead of the curve. If not, they really need to step aside. The topics are that critical."

"We are asking people to have a good understanding of data flow, controls, and governance."

Kathy Robinson

In Sanders' experience, however, it can be difficult to find someone with working IT knowledge who wants to be an auditor. "Many entry-level auditors have a desire to learn IT, or they have an IT background but no audit experience," he says, blaming, at least partly, "a failure to sell the important role an IT auditor plays."

If the in-house expertise is lacking, cosourcing may be a better option than assigning technical audits to unprepared practitioners. Robinson contracts with outside firms for expertise that she doesn't need—or can't afford—to have on staff full time.

BUILDING IT CAPABILITY

Indeed, issues around staffing an internal audit department and maintaining the right mix of generalists and specialists is one of a CAE's key IT challenges. Here is what internal audit leaders suggest for making sure every audit department has the IT know-how to get the job done.

Determine the Specialty Skills Needed "The desired IT skill set depends on the nature of the business one is auditing and the complexity of systems used," notes Mark Carawan, chief compliance officer with Citigroup in New York. "The larger and more complex the organization, the more likely it is that there will be a need for specialist skills to complement the deep business and product knowledge of the internal auditors following the end-to-end business processes."

The CAE, in consultation with senior business management and the audit committee chairman, should make that call. "The CAE should be working with management to understand the complexities of the business—such as robotics, process outsourcing, and cloud-based computing—and how customers use technology," Carawan says, "so the internal audit department can identify the risks to the business as a result."

Maintaining the right mix of generalists and specialists is a key IT challenge.

There will be a point as IT evolves, he adds, where someone is likely to say, "I'm not sure how this works. The

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

PREDICTIVE ANALYTICS

One specialist skill that increasingly is being used in audits is predictive analytics, which is mining data for meaningful patterns that can predict future trends and inform strategic planning, operations, and risk management. Already, internal audit departments use predictive analytics to strengthen audit coverage by quantifying issues to better understand the risks they are dealing with. There's no single solution; indeed, an analytics "toolbox" may be necessary for some large, complex organizations.

Predictive analytics is one of the reasons the audit team needs to be computer literate, says Citigroup's Mark Carawan. "The most successful auditors will know enough to say, 'This is an opportunity for predictive analytics and data mining to deliver control-enhancing assurance. Where am I going to have the greatest likelihood of a breach of policy, fraud losses, mispricing, or shortfalls in inventory?'" he explains. Carawan adds that it's important to have data analytics experts who are familiar with the latest tools and can interpret the results they produce.

"The desired IT skill set depends on the nature of the business one is auditing and the complexity of systems used."

Mark Carawan

audit department needs someone to explain that, as well as what the risks are and how we mitigate them." Be aware, though, that executives "may be reluctant to invest in adding more IT specialists to the third line of defense, beyond those already in the first and second lines," he says.

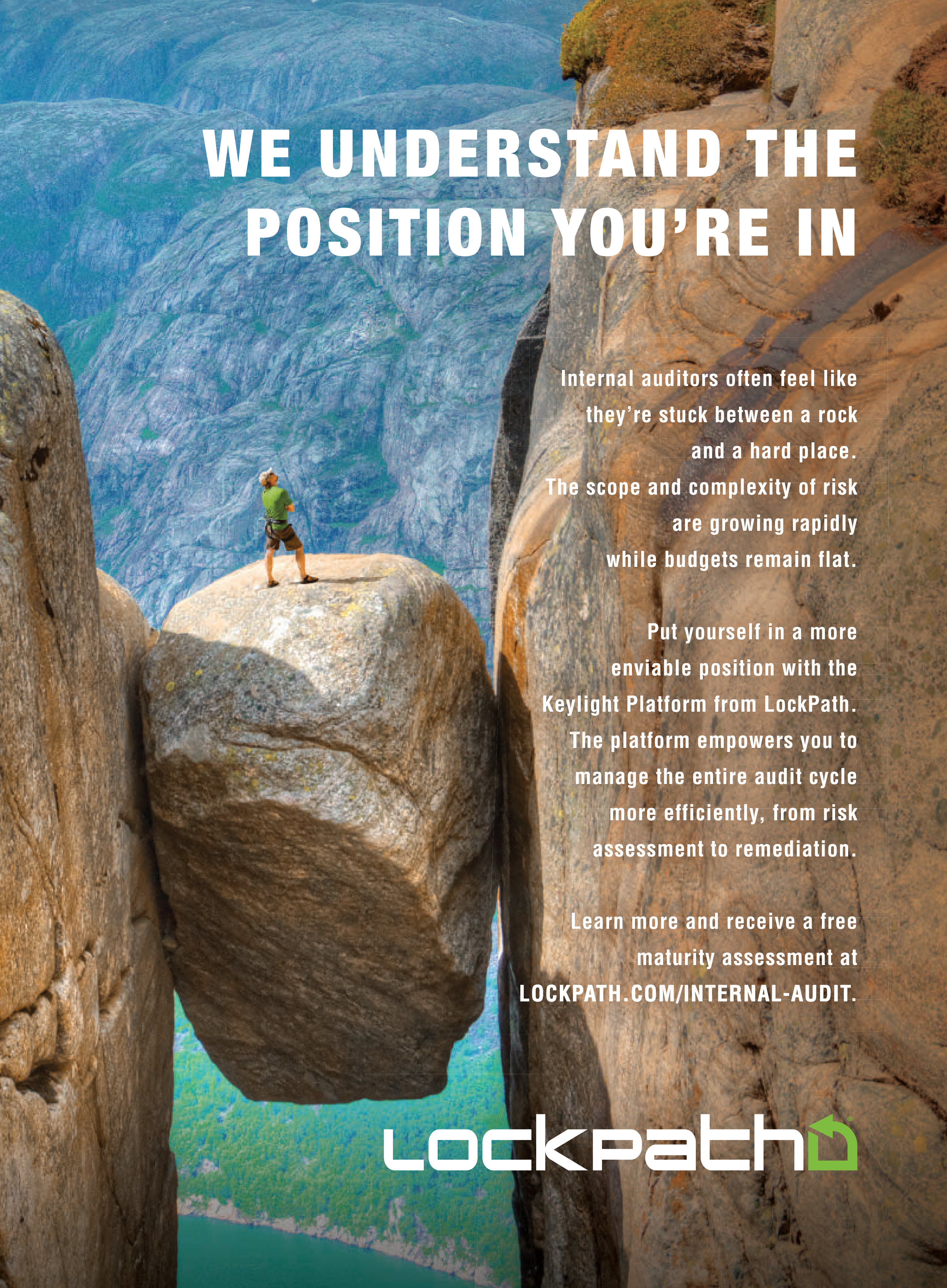
Make Adequate Education Available "Every audit department should have a formal training program to make sure the team is up to speed on both changes in IT risk and controls and changes in their company's IT landscape," Goschke recommends. Sanders agrees, noting that it's the CAE's job to "ensure adequate training is in place for auditors to stay current on IT trends and developments."

The basics should do it, Sanders says. "I don't expect every auditor to have in-depth knowledge," he explains, "just as I don't expect my IT auditors to understand the latest accounting pronouncements." Team members should seek out IT training, such as a seminar or conference, to build basic, solid skills, he advises, then start to specialize in a few specific areas over time.

Sanders recommends information sharing after every training event, "typically in the form of a summary presentation at an all-hands departmental meeting." He also maintains a spreadsheet in his department to track training hours. Although it may seem like IT skills get a lot of attention and require a lot of CAE input, it's unlikely any audit department is focusing too much on expensive IT expertise. "My audit shop has traditionally been heavy in IT auditors, but also heavy in IT risk," he notes. Indeed, there are many situations that demand the investment required to field a squad of IT experts.

Auditors should seek out IT training to build basic, solid skills.

Go Outside the Organization for Assistance "Auditors typically do not handle IT audits on their own, but they could supplement the IT audit team as additional arms and legs," Goschke comments. "Using an outside firm to come in for a day to train the team a


WE UNDERSTAND THE POSITION YOU'RE IN
Internal auditors often feel like they're stuck between a rock and a hard place. The scope and complexity of risk are growing rapidly while budgets remain flat.
Put yourself in a more enviable position with the Keylight Platform from LockPath. The platform empowers you to manage the entire audit cycle more efficiently, from risk assessment to remediation.
Learn more and receive a free maturity assessment at LOCKPATH.COM/INTERNAL-AUDIT.
Lockpath

THE AUTOMATED FUTURE

The precise menu of IT skills internal audit practitioners will need 10 years from now is anyone's guess. But it will likely refer to process automation. "Robotics and artificial intelligence will likely be much more prevalent in accounting and finance functions," Office Depot's Jennifer Goschke says. Some companies use "bots" to reconcile accounts, presenting audit challenges that don't exist with humans. "I can't go ask the bot a question about its process," she notes. "And how secure is it to have bots performing processes on sensitive data?" Citigroup's Mark Carawan adds: "Stakeholders and the businesses for which they are responsible will continue to seek automated solutions to achieve improved customer service and efficiency, enhanced risk management and control, and speedier execution."

few times a year is very cost-effective." Consulting firms also offer IT consulting and audit services on an hourly or project basis, she adds. Although this may be expensive, hiring someone full time with the same skills would cost even more. "Once my audit plan is determined for the year," she says, "I can decide which audit projects I'll perform with my internal team and which projects require specialized knowledge for which I should use an outside firm."

Audit departments probably won't be focused on the same issues three years from now, let alone 10.

Provide Big Picture Guidance and Clear Marching Orders "Overall, it's really a CAE's job to articulate the things that can impact the company's ability to execute strategy," Robinson states, "and to help make sure that the underlying IT infrastructure is adequate and operational by auditing for security, processing, and recovery, and providing that output to stakeholders." And although there is always some IT involved in their audits, she adds, "We could get lost in data analytics because there is so much we could do with it. My leadership team is responsible for homing in on the things that are most impactful."

COMPLETING THE JOB

Building IT knowledge and skills is a big job, but one that most internal audit departments should be able to accomplish. "It's challenging due to staff turnover and the ever-changing IT landscape," Goschke notes. "But the training is out there. You just need a plan."

But be careful about the "best laid schemes." Robinson says she is reluctant to guess what basic IT skills will look like 10 years from now. If she had tried 10 years ago, she would have been way off the mark. The iPhone was just being introduced in 2007, she explains, and "there's no way I'd have said we'd have a mobile app in 2017 that would be downloaded 11 million times—and that we'd have to audit mobile technology."

Indeed, audit departments probably won't be focused on the same issues three years from now, let alone 10. "Basic" will always be "basic," but the skills that audit leaders consider "basic" will always evolve. Ia

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

AUDITOR SPOTLIGHT

The University of South Alabama is a medical college with more than 16,000 students and it is here where we recently spoke with the college's Executive Director of Internal Audit, Robert Berry, to discuss his journey with data analytics. This is a snapshot of our conversation.

Q: How did you get started with data analytics?

A: Early in my career I was responsible for doing financial analysis for about a hundred retail stores, and I was using a spreadsheet program. I gathered the data I needed, and before I analyzed it I asked myself, "If I was the store manager, what would I want to see?"

So I analyzed the data manually and gave them what I thought they wanted. Next thing I knew they started requesting that I add more information to their statements. That's how it all started: being curious and trying to find answers to critical business questions.

I then moved to another organization, ditched the spreadsheets and migrated to a product that required a lot of SQL scripting. I taught myself just enough to be dangerous—which means I made a lot of mistakes. It was frustrating because I didn't have enough time to truly learn SQL.

I had an intern that was using IDEA in one of their classes, so we tried the educational version. We were in awe. We could point and click, then run simple queries right out of the box. No more complicated SQL. I've been hooked ever since.

Q: During which phase of the audit do you use your data analytics tool?

A: Data analysis can be done during any phase of the audit. At each phase you have to think about what your objective is and if the data is available. I would use data analytics during the planning phase as much as possible because it gives you the opportunity to get to know the area and formulate better questions before you get into the audit.

During the fieldwork phase, data analysis on an entire population leads to more accurate test results. Reports summarizing data analysis results provide greater fact-based audit findings. I tell people to always get the data because it tells a compelling story that no one can deny.

Q: How can auditors get management buy-in for data analytics?

A: My approach is to get the company as a whole to buy into the concept. It all boils down to three basic questions that I ask the leadership team:

1. Are you comfortable with all of the decisions you've made?
2. Do you believe you had the best information available to you prior to making those decisions?
3. When things go well or wrong, are you logically able to explain why?

If management can't answer yes to these questions, then they need to be using data to help them make healthier decisions. Data analytics is the key to moving us from irrational decision-making to strategic decision-making based on the results of logical analysis.

To learn more about how IDEA can improve your audits, visit us at www.casewareanalytics.com.

CASEWARE ANALYTICS


WE DON'T JUST FOLLOW RULES.
WE HAVE STANDARDS

Building
a data analytics program

Six strategies can facilitate progress when starting or furthering an analytics program.

**Gordon Braun,
Andrew Struthers-Kennedy,
and Gregg Wishna**

Illustration by Sean Yates

In today's data-hungry world, an analytics-capable audit function is a necessity. However, relatively few audit teams have developed sophisticated analytics capabilities and an embedded, integrated approach to analytics. So how can internal audit functions initiate and advance their analytics capabilities? Internal audit functions that have successfully implemented sustainable analytics activities have not only been able to clearly visualize and articulate the value analytics can deliver to their functions and the broader business, but also have started to realize that value in enhanced efficiency, effectiveness, and risk awareness.

Along the way, many functions have experienced missteps and setbacks. The lessons they have learned should benefit internal audit departments embarking on their own analytics journeys or those attempting to overcome false starts of the past. Some of these hard-earned insights are what one might expect. Difficult access to enterprise data stores marks a widespread pitfall, as does insufficient planning. Other data analytics lessons will surprise the uninitiated. Investing in robust technical skills training and analytics tools implementation often can be a distraction to getting an analytics program off the ground. By knowing what to avoid, internal audit departments can keep a data analytics program on track to reach its full potential.

TOOLS FOR SUCCESS

When internal audit leaders commit to introducing or furthering a data analytics program, there are six strategies that can positively impact these initiatives.

1 Create awareness rather than a silo

Internal audit leaders should resist the inclination to start by creating a data analytics silo within the larger function. While dedicated analytics functions are present within many internal audit functions with advanced analytics capabilities, this structure should more appropriately be treated as a long-term goal or possible target state than an immediate to-do item when getting started.

While it is necessary to have the appropriate technical competence within the team, creating a silo structure from the start can reduce focus on a more important driver of success: data and analytics awareness. This mindset helps internal auditors understand how data is created, processed, and consumed as it flows throughout the organization, the key systems where it resides, and the key business processes and decisions that it supports. This understanding represents a business-centric view of analytics as opposed to a technology-only view, a critical distinction in developing the right kind of thinking among the internal audit team.

When an internal audit function decides to reassign a technical resource as the team's analytics champion, problems often ensue. Creating this type of structure too soon can cause the rest of internal audit, as well as the business, to view audit analytics as a purely technical exercise as opposed to an integrated component of internal audit's culture, strategy, and activities. Insight from analytics are the result of the intersection between business awareness and the application of analytics tools and methodologies. These are two sides of the same coin and both must be present for success.

Internal audit leaders also should reflect on how they source their analytics talent. While there is no one way to do this, leaders should recognize that hiring analytics professionals or repurposing technical resources can pose risks to the development of an analytics mindset throughout the entire internal audit team. It takes time to understand business processes and what valuable information can be gleaned from the systems and data that underpin them. Building a more pervasive analytics mindset across the internal audit department is critical. The most effective audit analytics programs operate in a tightly coordinated—if not seamless—manner with all other parts of the audit team. All members of the team think about the data that exists in the environment, its business relevance, and the stories it can tell. The analytics teams then layer in their view and capabilities.

Building a more pervasive analytics mindset is critical.

Dedicated analytics functions and externally hired analytics experts are common hallmarks of top-performing analytics capabilities; however, neither of these elements should be used in place of the initial establishment of the right analytics mindset throughout the internal audit function.

2 Understand the data before investing in a tool

One of the most common start-up lessons involves resisting the desire to acquire the latest and greatest analytical tool. Given the impressive power, look, and feel of analytics tools, it's difficult to not be sold on a new piece of software with the promise that, within hours, internal audit will be generating a flurry of queries and new intelligence insights.

Rather than a first step, however, implementing an analytics tool should be a more deliberate step in the rollout of an analytics program. A rush to start using these tools, without establishing a plan and set of initial, high-value use cases, often leads to results that lack business impact, which can be detrimental for a start-up analytics activity.

Before using a tool, internal auditors should carefully evaluate a high-value area to target, understand the data source, validate it, and identify how the results will be evaluated and shared. When it comes to analytics tools, it is helpful to adhere to the 80/20 rule: 80 percent of the analytics team's work should consist of understanding the data, the business process it supports, and the activities and decision-making that it drives, along with the business value the analysis is designed to deliver; 20 percent of the effort should focus on the technical aspects of the analysis, including the audit tool.

3 Plan sufficiently

Too many analytics initiatives suffer from too little planning. Plunging into

Two-thirds of internal audit functions are using data analytics as part of their audit process, according to Protiviti's 2017 Embracing Analytics in Auditing survey.

INSIGHT, EFFICIENCY, AND VALUE

The growing demand for internal audit's data analytics services stems, in large part, from the benefits these offerings have delivered. Analytics help internal auditors execute the audit plan more efficiently, allow them to quantify and more effectively communicate the impact of findings, generate additional insights concerning risks, and identify new opportunities to drive business value. Internal audit teams that invest appropriately are using analytics to proactively identify fraud, waste, abuse, performance variances outside acceptable boundaries, previously unidentified risky behaviors, data quality issues, unauthorized access, and a host of other items for management's consideration. Some internal audit functions even hand off analytics solutions to business partners who are eager to incorporate them into their own processes to monitor for key performance and risk indicators.

data analytics does not mean that internal audit functions should give short shrift to key planning considerations.

The most effective and sustainable analytics programs tend to begin with a planning effort that includes:

- Understanding the system and data landscape; how data is created, processed, and consumed; and how it drives business activities and decision-making.
- Educating internal auditors on the power, benefits, and applications of audit analytics (the analytics mindset).
- Laying out how analytical talent will be trained or hired and retained.
- Seeking business partners' input on areas of their domains that might benefit from audit analytics.
- Carefully identifying which initial analytics are likely to yield the most valuable results—and, as a result, support from business partners.

Neglecting any one of these items can lead to initial results that are low impact or miss the mark entirely.

When educating internal audit team members about the use of data analytics, it is helpful to steer the focus away from the technical inner workings of the capability by presenting real examples that demonstrate how analytics enhance the efficiency, effectiveness, or risk awareness of the internal audit function and the broader organization (i.e., how data can be turned into information that provides risk and business insights).

4 Think big picture

The expansive reach of audit analytics has, oddly enough, resulted in narrow thinking about its application. For years, internal audit professionals and experts have marveled at the way analytics and continuous auditing techniques can be deployed to test massive populations of transactions. This capability is rightly trumpeted as a massive improvement over the traditional approach of manually sampling large data sets, often months after the associated activity has occurred, to identify problems. While accurate, this view of analytics is severely limited.

Leading internal audit functions now use analytics throughout the audit life cycle to support dynamic risk assessments; monitor trends, fraud, and risk and performance indicators, or deviations from acceptable performance levels; and model business outcomes. These functions tend to view analytics as a way to interpret data that helps tell a story to the business that may not

MORE

Visit our Mobile app + InternalAuditor.org to watch a video on enhancing internal audit with data analytics.

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

have been told before. To be successful here, there has to be an acute understanding of the data that is created, processed, and consumed within—and across—the organization and how it is used to drive business activity and decision-making.

5 Partner with IT

Given that data typically exists in a multitude of different systems throughout organizations as well as within third-party (e.g., cloud) environments, internal audit frequently encounters difficulties when attempting to access data for analytics. This problem relates not only to accessibility (the protracted data request process with IT), but also to completeness, accuracy, and validity of the data. Without understanding the specifics of what they are asking for, internal auditors cannot reasonably expect to get what they need—at least, not the first time around. In some cases, lengthy and ineffective data request back-and-forth between internal audit and IT departments results in data integrity issues (at best, perhaps) or the planned analytic being canceled entirely.

A picture is worth a thousand words. The same principle applies to the presentation of the analytics results.

To succeed, audit analytics teams need to partner with IT departments to develop a robust process for data acquisition—either through specific and easily understood data requests or through direct connections to data repositories. This all starts by understanding the data environment. While this marks a common goal, it takes time, effort, and coordination to get there. Auditors should consider discussing how to decide which data elements should be created and captured, the business rationale for doing so, and how internal audit and business partners will use the information that analytics produce.

Thanks to recent advancements, current analytical tools more easily integrate with other enterprise systems. Internal audit functions' growing tendency to use dedicated data warehouses also helps address data access and quality challenges, which can reduce stress on business production systems by giving internal auditors their own sandbox to play with data. However, there are risks with this approach, particularly with regard to security and privacy. Ultimately, establishing a dedicated data warehouse requires a sound business case that, among other things, addresses these risks.

Other, less technical qualities and practices also come in handy. Internal audit functions that have earned a reputation for collaborating with the business consistently encounter fewer data management obstacles when deploying data analytics. Their success stems partly from the fact that collaborative internal auditors are more apt to learn about, and apply, data governance standards and practices from their IT colleagues, which can help ease access to quality data residing in systems scattered throughout the organization.

6 Take advantage of visualization tools for inspired reporting

A picture is worth a thousand words. The same principle applies to the presentation—or visualization—of the analytics results. Tabular formats and simple charts are a thing of the past. Analytics reporting packages should

58% of respondents who **regularly use** data analytics report that poor data analytics design caused extra work, according to the Audit Executive Center's 2017 North American Pulse of Internal Audit Report.

be making use of widely available visualization tools. These tools allow for the dynamic presentation of results (e.g., a country map that shows the top locations where purchase card spending occurs) and real time, drill-down capability that represents a far cry from the static analytics presentations of the past. Visually compelling, high-impact reports can help internal audit's clients quickly draw insights from the data.

A FUNDAMENTAL SHIFT

At present, data is being created and collected at a pace that is far beyond anything seen before. While there is always some risk in undertaking a new program—and a desire to prove the return on investment—the bigger risk is doing nothing. It is simply not an approach that internal audit functions can afford to take if they want to keep up with the business, stay relevant, and deliver value and insight. The most innovative companies are looking at ways to capture and use data to transform their business operations as part of digitalization initiatives. Internal audit must be equally innovative and embracing of the need and value to make the company's data work for them.

A key method to overcome common time and resource constraints with setting up a discrete analytics group within internal audit is by focusing on an "analytics mindset." Further, internal audit functions are encouraged to work with business partners to identify areas where analytics can have high impact and high value, provide real business insight, and help address business challenges (rather than focus on a return on investment calculation). The value delivered in these initial analytics projects will set the stage for the program. Internal audit should look for parts of the business that are particularly data dense, or that have high volumes of data processing but still rely heavily on manual procedures. For example, focus on ways to:

- Pull business insight from the data-heavy areas (and show management a story they have not seen before).
- Work with management to convert audit analytics into reports that can be used in place of time-intensive procedures (e.g., "real time" monitoring of large, disparate data sets for key fraud indicators).
- Quantify the impact of findings and deliver more insight through audit reports.

These are some of the ways that internal audit functions are able to quickly demonstrate and communicate value in their investment in, and use of, analytics. Ultimately, however, stakeholders must recognize that there is a fundamental shift in how business is being conducted, and as such auditors must match that with a fundamental shift in how they audit.

EACH JOURNEY IS UNIQUE

Establishing a robust analytics program may take several years to mature. The process for developing a data analytics capability tends to be unique for each internal audit function. Some standard general assessments exist and can help, but each internal audit leader should chart a path forward that reflects the unique qualities and needs of his or her function and the unique characteristics of the industry, the organization, and the team's relationships with business partners. Ia

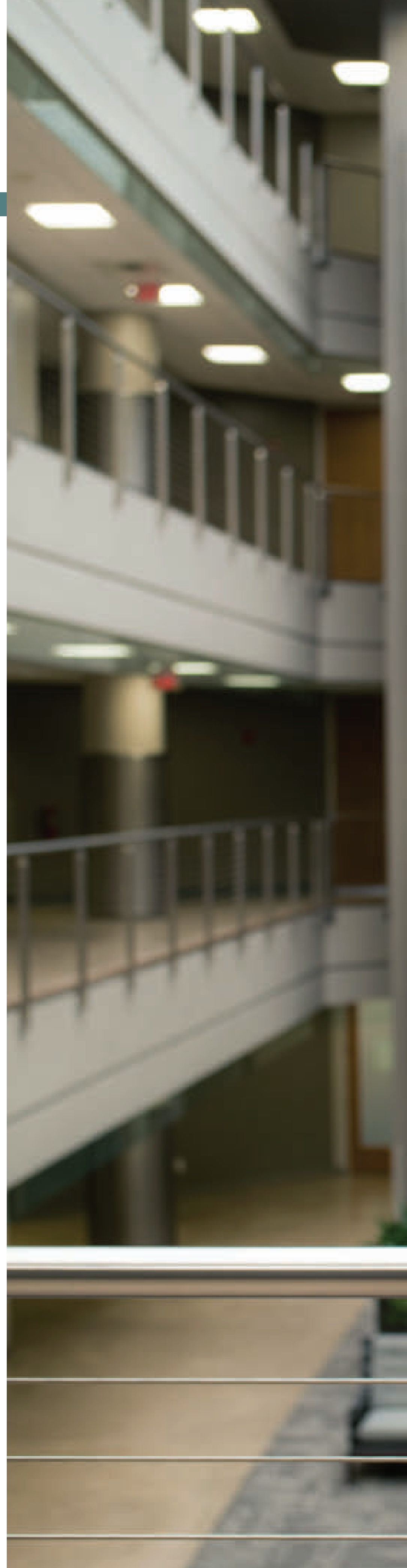
GORDON BRAUN, CIA, CISA, CGEIT, *is a managing director at Protiviti in Minneapolis, Minn.*

ANDREW STRUTHERS-KENNEDY, CISA, *is a managing director and global lead of IT Audit at Protiviti in Baltimore.*

GREGG WISHNA, CISA, *is an associate director at Protiviti in Atlanta.*

MORE

For additional guidance, VISIT http://bit.ly/2u6iVQv to download GTAG: Understanding and Auditing Big Data.



As ubiquitous as social media is today, it is hard to recall a time when we were not glued to our Facebook, Twitter, or Instagram accounts. Indeed, it is rare to read about a cause or event without running into at least one hashtag. This article is no exception.

As the 2017-2018 global chairman of The IIA Board of Directors—a privilege I am humbled and honored to experience—one of my first assignments was to develop a theme for my term. Coming up with the basics was easy: Purpose, service, and impact are three concepts that are very important to me. But when I looked at those words on their own, they seemed somehow incomplete. Then, as I was bouncing ideas off my team, the hashtag treatment was suggested. Thus, my theme became #PurposeServiceImpact.

We have become so accustomed to the hashtag, we often forget what it is intended to convey. It's a useful, shorthand way to say, "pay attention," "join the discussion," and "pass it along"—reactions I hope IIA members have to the concepts of *purpose, service*, and *impact* as we go through the year, because I believe they have a very real place in our personal and professional lives.

#PURPOSE

Purpose is fairly straightforward. We all have a sense of purpose about our careers and our lives. It is the "why" of what we are doing, our mission, the reason we want to make a difference. As individuals, we need to know that all of the effort, focus, and sacrifice we have invested over time will pay off in achieving a goal.

As internal auditors, our mission is clearly laid out for us in The IIA's International Professional Practices Framework: "Enhance and protect organizational value by providing risk-based and objective assurance, advice, and insight." How we enhance and protect organizational value is different for each of us based on our organization's business. Is it market share? New products? Students educated? Patients served? Perception of reputation? Earnings per share? Whatever it is, internal auditors, at the very least, help management maintain that value, but, ideally, we enhance and increase it through the work we do.

As individuals and as internal auditors, we do not operate in a vacuum. We function within some sort of larger construct. As individuals, that may be a family, a community, a club—even an organization such as The IIA. As internal auditors, it is where we work. We must clearly understand the purpose of our organization and be certain that our personal sense of purpose aligns with it. Generally, every organization has a mission statement, but studying other indicators such as culture, strategy, and reputation can provide useful information, as well. Then we must determine how we can help the organization realize its mission.

A practical application can be found in the way some auditors are evolving the traditional risk-based audit approach—which is still very valuable—with

#PurposeServiceImpact

The IIA's 2017-2018 Global Chairman of the Board J. MICHAEL PEPPERS encourages internal auditors to unify around the three concepts in his powerful hashtag.

Photographs by Darren Carroll

more strategic elements. Start with the big-picture objectives of the organization and take the risk assessment from there. This helps ensure that what internal auditors do is more strategic and supports the goals of the organization—its purpose. For example, I once audited an area that had wonderful ideas, plans, and goals, but lacked good project management to address those plans in a systematic and metrics-driven way. I provided recommendations about managing projects. This was not a typical risk audit, but it provided value: The department recognized that adding this element would help in achieving departmental goals.

For almost 10 years, I worked on a university campus, and nearly every day I would walk on the sidewalks with the students we were educating. For another 15 years, I worked at two of our academic medical centers where I would walk the halls and see the patients we were serving. I came face to face with real stakeholders—the people who are counting on the organization—and that connection has always given me the drive to do all I can as an internal auditor to help my institutions succeed in their missions.

#SERVICE

Service is purpose put into action. It is doing things to meet the goals expressed in mission statements, transitioning purpose from concept to reality. Consequently, it can be the hardest part of the #PurposeServiceImpact trilogy. Purpose identifies noble goals and impact represents the outcomes of actions completed to achieve those goals. Service is the link between the two; it is "walking the walk."

It is often said that internal auditors should "know the business" to be as effective as possible, and there is no question it is important to establish credibility with clients. At one point in my work at a health institution, I became aware that a health-care administrator certification was valued by many of the hospital leaders, so I decided to prepare for and take the certification exam. It demonstrated to my colleagues that I knew and cared about our business, and was willing to "walk the walk" to make us successful.

Internal auditors certainly do not lack opportunities to serve. Almost daily, we encounter areas where unsurpassed service is required or expected. According to the stakeholders represented in The IIA's 2017 North American Pulse of Internal Audit, we must embrace our role as educator and change agent; be brave enough, even in the face of professional or personal danger, to do the right thing; avoid viewing the world in black and white; develop strong relationships with stakeholders; build interpersonal skills; and continue to develop competencies. This list goes well beyond *what* we are expected to do. It outlines expectations for *how* we do it, as well.

It's no wonder we sometimes feel like we are on a tightrope stretched across a gaping canyon. We know we must perfect our balancing act to face the risks and service expectations ahead—not only at work, but also at

#BoardPriorities

During the coming year, I anticipate deploying the #PurposeServiceImpact philosophy as I lead The IIA's Global Board of Directors in several initiatives:

- Addressing the recommendations of a special Governance Task Force that has studied The IIA's governance structure and processes. Significant changes are being proposed to the board and membership.
- Completing the triennial refresh of The IIA's global strategic plan. A new approach to gather input from multiple regional sessions is underway.
- Advancing the recent Guiding Principles of Effective Affiliate Governance, which is intended to help affiliates serve their stakeholders and more than 190,000 members worldwide.
- Studying laws, regulations, and questions related to licensing the internal audit profession. A global steering committee is working on this project.
- Considering ways to increase the level of conformance with the *International Standards for the Professional Practice of Internal Auditing*.
- Assessing The IIA's portfolio of certifications to ensure it meets stakeholder expectations and is positioned for sustained success.

home, with friends, and in our outside activities.

It is in those optional activities where many of us find another way to serve: volunteering. I believe volunteering is one of the most powerful manifestations of service because there is nothing that makes us do it. We do it freely and willingly.

There are many reasons to volunteer. We want to get to know a community, gain leadership skills, feel needed, do our civic duty, learn something new, be challenged, do something different from what we do at work, make new friends, be part of a team, test ourselves, build our resume, give back, or feel good.

Volunteering helps us in our profession, as well. Well-rounded internal auditors recognize the benefits of understanding the enterprise end to end. To gain that understanding, we have to raise our heads up from our desks and see what is happening on a broader basis. We need to get out of

> "The best and most successful internal auditors I know understand that internal auditing is more than just a job; it is a sincere effort to improve the lot of others, whether organizations or individuals."

VISIT our Mobile app + InternalAuditor.org to watch a video of J. Michael Peppers discussing his chairman's theme, "#PurposeServiceImpact."

our offices—and our comfort zones. Volunteering provides that opportunity.

Those who are new to volunteering can start small. My long history of volunteering with The IIA began with being a greeter at meetings. I did it to help my local chapter, but that was only part of the reason. I also wanted to help myself advance both personally and professionally. That position made it easy for me to expand my network. Small steps can lead to big destinations; I am a case in point.

Of course, sometimes our services are needed in positions that may not be our first choice. When that happens, we can take a longer-term view. Fortunately, we can usually learn from any situation and gain the satisfaction of contributing to the greater good. Hopefully, those less-than-perfect volunteer roles are the exception rather than the rule. Life is short. When you have the choice, choose to make a difference in things that matter to you.

#IMPACT

And now we arrive at impact—the destination of the journey, the reason we provided service, and the realization of our purpose. The best and most successful internal auditors I know understand that internal auditing is more than just a job; it is a sincere effort to improve the lot of others, whether organizations or individuals. But it is not an activity that provides immediate, easily seen impacts. We often have to examine the ripple effects our efforts leave behind. Take for example two statistics from The IIA's Pulse report: In 2016, 29 percent of respondents reported an increase in internal audit staff, and 30 percent expected to add staff in 2017. This is a ripple effect of the impact of internal audit. Today's cost-conscious boards and executives would not spend substantially more on risk, control, and governance processes unless they were realizing value. We are making an impact.

We have to choose where we will make an impact. Given our time, energies, and resources, we need to focus on areas that enable us to influence things that are important to us and that we will look back on with pride.

For me, it is always education. Being in the higher education system, a financial supporter of The IIA's Internal Auditing Education Partnership program, and a regular speaker in professional and college programs, I am a believer in the value and importance of education. Several years ago, in the early days of data analytics, I had an

"For me, it is always education."

#HigherEdFocus

In my position as chief audit executive (CAE), I support the Board of Regents and executive management at the expansive University of Texas System. The System has more than 120 internal auditors at its 14 academic and health science institutions, consisting of more than 220,000 students, 100,000 faculty and staff, and an operating budget of almost $18 billion.

My career-long focus in higher education started in graduate school at the University of South Florida where I was the student internal audit intern. After earning a Master of Accountancy, I spent time in public accounting before returning to the university to lead that same internal audit department for almost 10 years. In 1999, I moved to Texas and was the CAE at UT Medical Branch in Galveston and UT MD Anderson Cancer Center in Houston before arriving at UT System Administration in 2013.

I proudly admit to being a "career internal auditor." I can probably count on one hand the times I've done what would be considered a "repeat" audit. Because our organizations continually change, so do our audits. There's nothing routine, cyclical, or boring about what we do.

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

audit manager who was particularly good at analytics, which we used to achieve real wins in audit engagements. But we had a vision for even greater impact. Because we worked in a university setting, we were regular guest speakers in the audit classes and we knew that students were not getting exposure to data analytics tools. So, we convinced audit faculty that the curriculum needed to include this important aspect of practical auditing, and we engaged a software provider to make its tool available for this academic purpose. Since then, other auditors, faculty, and vendors have done the same, truly impacting the preparation of students for the audit workplace.

PUTTING IT ALL TOGETHER

Our lives have a lot of distractions, but I have an easy way to keep our eyes on the goal of creating appropriate impact. Think of the process as an equation—a simple set of steps:

1. *If we understand the purpose of the organization or profession…*
2. *And our own purpose within that group…*
3. *And those purposes are aligned…*
4. *And if we commit to providing excellent, competent, ethical service…*
5. *We will have an impact. We will make a difference.*

The #PurposeServiceImpact hashtag has a specific use, one I hope will resonate with IIA members. It says I would like you to think about these three concepts, identify with them, unify around them, and connect them with your own thoughts or activities. Twitter has shown the world how powerful the hashtag can be as a means to rally people around specific goals. I would like to think we can do the same within The IIA. Ia

J. MICHAEL PEPPERS, CIA, QIAL, CRMA, *is the chief audit executive of The University of Texas System in Austin.*

#FaithFamilyFlowers

Outside my professional life, I have three priorities that keep me grounded and rounded: faith, family, and flowers. Faith is the most important aspect of my life, providing the foundation for actions and decisions both personal and professional. It is also a constant footing for me as I assess my own purpose, service, and impact. Next comes family: I have two adult daughters and two granddaughters who are never far from my thoughts, even if a bit too far away physically for my liking. I rely on video technology to "see" them as much as possible.

My family may, however, quip that they compete for my attention with another of my loves: my daylilies. As an internal auditor, I have not been afraid to dig deep and get my hands dirty, and the same goes for my garden. When I moved to Texas in 1999, a co-worker introduced me to daylilies. I started with 10 plants and grew to as many as 500 varieties in my yard at one time. In my new Austin garden, I'm down to *only* about 200 varieties. My passion goes beyond weekend gardening; I have won competitive flower shows, and my garden recently was designated by the American Hemerocallis Society as an official display garden. In addition, the garden was recently a stop on three different garden and pond tours.

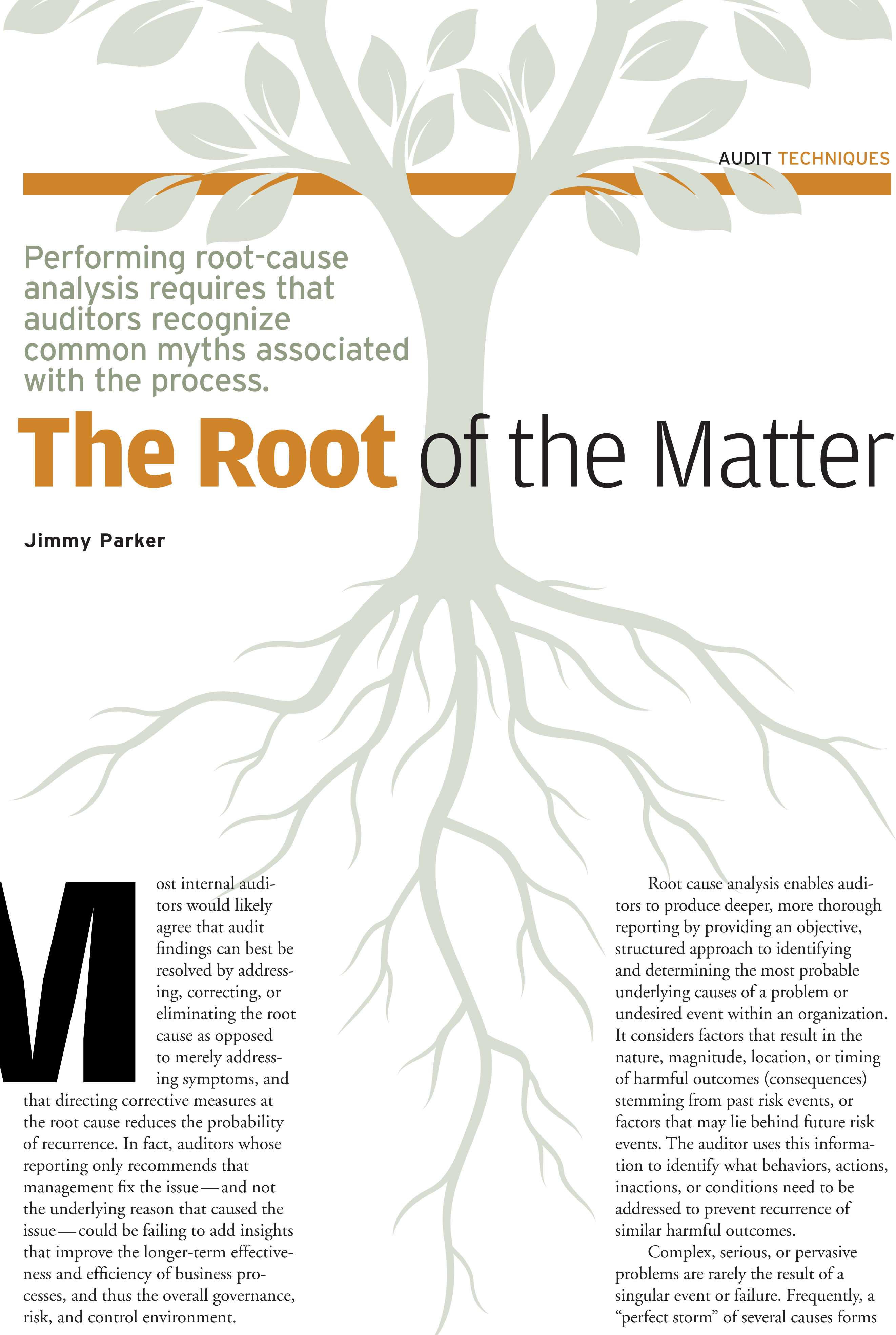
I have a shirt that states, "Gardening… it's cheaper than therapy." While I admit that outdoor work is a source of therapy for me, I do not concede that it's less expensive!

"Gardening… it's cheaper than therapy."

PHOTOS (2): COURTESY OF MIKE PEPPERS

Performing root-cause analysis requires that auditors recognize common myths associated with the process.

The Root of the Matter



Jimmy Parker

Most internal auditors would likely agree that audit findings can best be resolved by addressing, correcting, or eliminating the root cause as opposed to merely addressing symptoms, and that directing corrective measures at the root cause reduces the probability of recurrence. In fact, auditors whose reporting only recommends that management fix the issue—and not the underlying reason that caused the issue—could be failing to add insights that improve the longer-term effectiveness and efficiency of business processes, and thus the overall governance, risk, and control environment.

Root cause analysis enables auditors to produce deeper, more thorough reporting by providing an objective, structured approach to identifying and determining the most probable underlying causes of a problem or undesired event within an organization. It considers factors that result in the nature, magnitude, location, or timing of harmful outcomes (consequences) stemming from past risk events, or factors that may lie behind future risk events. The auditor uses this information to identify what behaviors, actions, inactions, or conditions need to be addressed to prevent recurrence of similar harmful outcomes.

Complex, serious, or pervasive problems are rarely the result of a singular event or failure. Frequently, a "perfect storm" of several causes forms

ROLANDTOPOR / SHUTTERSTOCK.COM

to create an ideal environment for the failure to occur. Moreover, simply getting to the root cause to prevent it from happening again may not be enough—the consequences have to be addressed.

To better understand root cause analysis, two general myths need to be dispelled—the myth of the single root cause, and the myth that fixing the root cause alone fixes the problem. Upon recognizing these false notions, internal auditors can use several methods to perform root cause analysis more effectively on their engagements.

Focusing on a single root cause can limit the solutions set.

MULTIPLE ROOT CAUSES

Many organizations mistakenly use the term *root cause* to identify one main cause. However, focusing on a single cause can limit the solutions set, resulting in the exclusion of viable solutions.

Internal auditors commonly use the Five Whys technique to explore the cause–effect relationships underlying audit issues, with the goal of determining the root cause of a defect or problem. By asking successive "why" questions, the nature of the problem as well as its solution usually become clearer. Asking "why" helps identify the causes associated with each sequential step of the defined problem or event. An example from The IIA's Implementation Guide 2320: Analysis and Evaluation illustrates this technique: "The worker fell. Why? Because oil was on the floor. Why? Because a part was leaking. Why? Because the part keeps failing. Why? Because the quality standards for suppliers are insufficient." By the fifth "why," the internal auditor should have identified or be close to identifying the root cause.

Although this technique can be useful, some experts contend that using the Five Whys leads auditors to mistakenly believe that only one true root cause to an issue exists—and that if they are successful in finding that root cause they will permanently solve the problem. In reality, several related or unrelated root causes are frequently responsible for the findings that auditors identify.

Rather than assuming the presence of just one root cause, internal auditors should brainstorm with a team to identify all the potential causes that contribute to a problem. The process can result in multiple opportunities to mitigate risk and prevent problems from occurring. It is also helpful for auditors to think about root cause analysis in terms of three stages: identification, measurement, and prioritization. Using this approach, the structure of root cause analysis is analogous to the structure of a risk assessment (see "ERM vs. Root Cause" on this page).

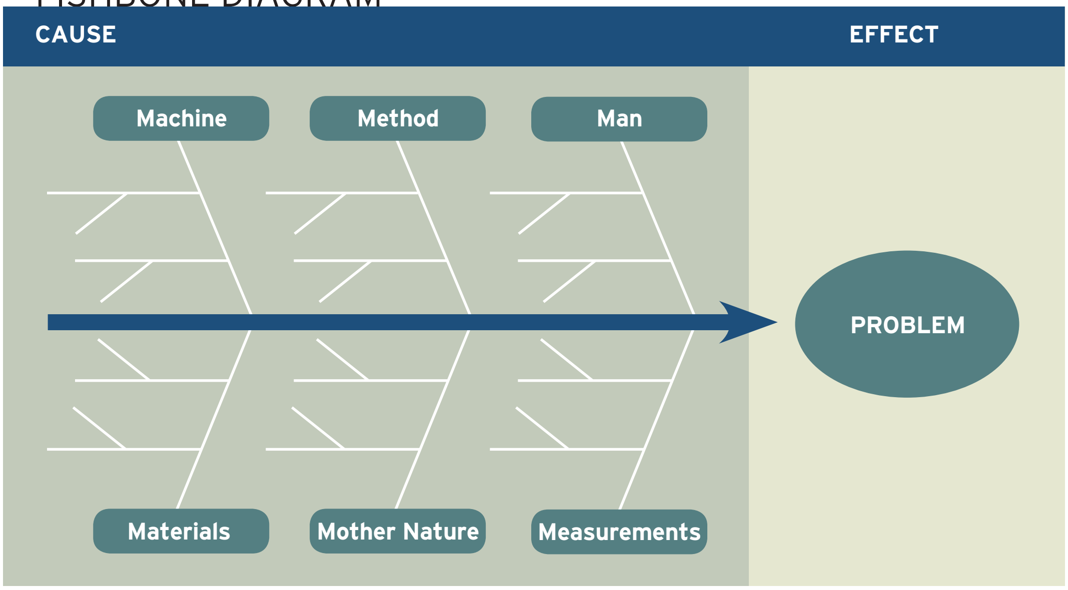
Identification The cause-and-effect diagram represents a preferred tool for identifying multiple root causes. Also called a fishbone diagram—because its shape is similar to the side view of a fish skeleton—this method enables users to visually display the many potential causes of a problem or an effect, helping reveal key relationships among causes and provide additional insight into process behavior. It uses a graphical description of the process elements to analyze potential sources of process variation (see "Fishbone Diagram" on page 55).

ERM VS. ROOT CAUSE

ERM	ROOT CAUSE ANALYSIS
1. Objective	1. Problem
2. Risk(s) a) Identification b) Measurement c) Prioritization	2. Root Cause(s) a) Identification b) Measurement c) Prioritization
3. Risk Response	3. Recommendation/Management Action Plan

“Root cause-based action plans are ideal, as they mitigate the underlying cause of the condition that triggered the observation.” – IIA PRACTICE GUIDE: AUDIT REPORTS

FISHBONE DIAGRAM



When using a team approach to problem solving, differing opinions often arise as to the problem's root cause. The fishbone diagram helps capture these ideas and stimulate team brainstorming. It also can be used to structure the brainstorming session, as the diagram not only helps identify the many possible causes for an effect or problem, but also enables users to sort these ideas into useful categories:

- Man (people) — anyone involved with the process.
- Machine (equipment/technology) — any equipment, software, hardware, tools, supplies, etc. required to accomplish the job.
- Measurements (management) — data generated from the process and metrics used to evaluate its quality, efficiency, and effectiveness.
- Method (process) — how the process is performed and the specific requirements for doing it, such as policies, procedures, and rules.
- Materials (inputs) — raw materials, parts, documents, data, etc. used to produce the final product or output of the process.
- Mother Nature (environment) — the conditions, such as location, time, and temperature, in which the process operates, as well as external factors that are not associated with the natural environment, including laws, regulations, and culture.

Causes derived from the brainstorming effort are grouped into these categories and then traced back to the root causes, which can be performed using the Five Whys technique in conjunction with the fishbone diagram. Because people by nature often like to start working on a problem as quickly as possible, this approach can help yield a more efficient and thorough exploration of the issues behind the problem, which in turn will lead to a more robust solution.

Measurement and Prioritization

For the measurement and prioritization phases, the team can numerically confirm

MORE

VISIT InternalAuditor.org for additional resources, including a variant of the Five Whys technique that better accommodates multiple root causes.

the proportion of each root cause's impact on the problem and rank them accordingly. Two root cause analysis tools can be especially useful in this process—the Pareto chart and the scatter diagram.

The Pareto chart illustrates the Pareto principle, frequently referred to as the 80/20 rule, which states that

Scatter diagrams pair causes and effects to look for relationships.

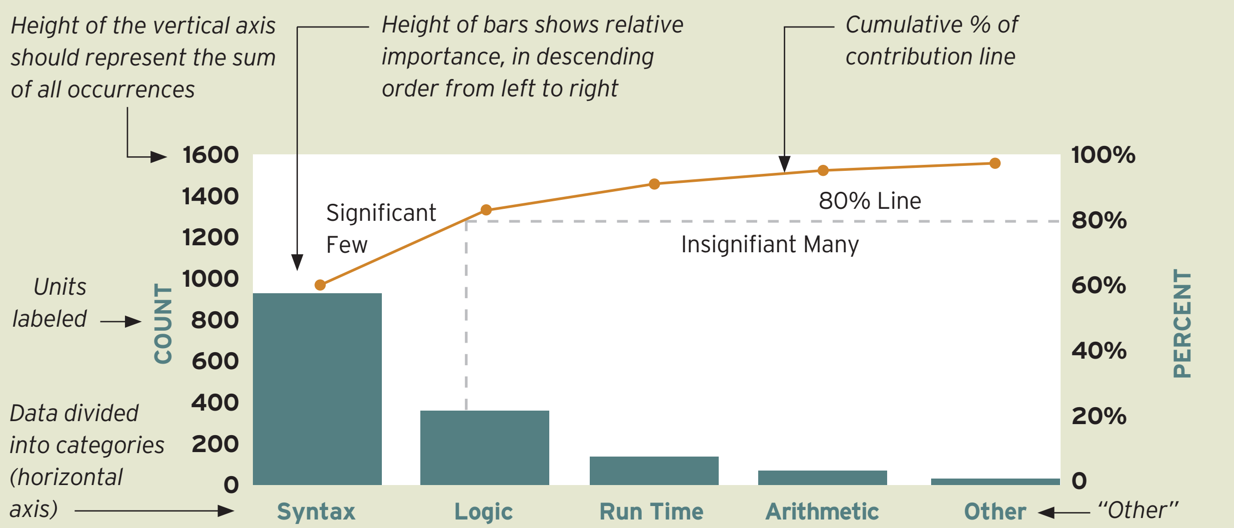
20 percent of the population accounts for 80 percent of the phenomenon. The chart's purpose is to highlight the set of factors or activities that most contribute to a problem or opportunity (see "Pareto Chart — Types of Errors" on this page).

By categorizing and displaying the supporting data for multiple causes, the Pareto chart can focus attention on the causes most important to resolving, reducing, or eliminating a problem. This approach can be particularly helpful when the team is:

- Analyzing data about potential root causes or the frequency of problems.
- Dealing with many different problems and causes but looking to focus on the most significant ones.
- Analyzing wide-reaching causes by zeroing in on their individual components.

Scatter diagrams pair causes and effects, with one variable on each axis, to look for a relationship between them. It could depict the relationship between a cause and an effect, between one cause and another, or even between one cause and two others. If the diagram reveals a relationship, then the possibility arises that one variable may be controlled by varying the other variable, or that two effects that appear related share the same cause. During root cause analysis, scatter

PARETO CHART – TYPES OF ERRORS

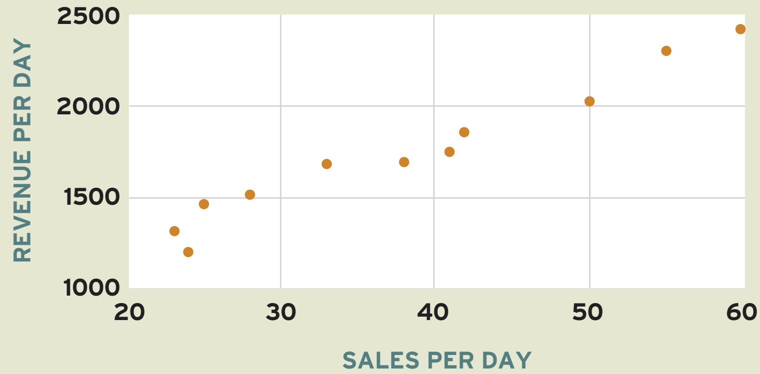


	Syntax	Logic	Run Time	Arithmetic	Other
Count	950	365	125	60	30
Cumulative %	62.1%	85.9%	94.1%	98.0%	100.0%
%	62.1%	23.9%	8.2%	3.9%	2.0%

"When conducting a root cause analysis, internal auditors must exercise due professional care by considering effort in relation to the potential benefits." – IIA IMPLEMENTATION GUIDE 2320: ANALYSIS AND EVALUATION

SCATTER DIAGRAM – REVENUE VS. SALES

SALES PER DAY	REVENUE PER DAY
23	1312
24	1205
25	1455
28	1513
33	1678
38	1691
41	1739
42	1852
50	2015
55	2294
60	2413



diagrams can be useful for displaying and analyzing the relationship or correlation between cause and effect variables, which can help point to the true root causes of problems as well as facilitate ranking those causes in order of importance by strength of relationship (see "Scatter Diagram—Revenue vs. Sales" on this page).

FIXING THE PROBLEM

Once internal auditors have identified a root cause, or multiple root causes, they must be able to offer meaningful recommendations or management action plans to address the issue. But contrary to a common misconception, fixing the root cause alone does not necessarily fix the problem—auditors must also help address the damage or difficulties that emerged as a result. To better understand this idea, practitioners can benefit from reviewing a key foundational concept in audit report writing, informally referred to as the Five C's:

- » Condition (*what is*).
- » Criteria (*what should be).*
- » Cause (*why*).
- » Consequence [Effect] (*so what*).
- » Corrective action plans and recommendations (*what's to be done*).

Well-written audit reports provide recommendations that address the underlying root causes of a problem, thus helping to ensure the condition will not recur. Because recommendations must resolve both the condition and the cause, the terminology used in the recommendation often mirrors or matches the terminology in the condition and the cause. Moreover, the recommendation must identify the action necessary to bring the condition in line with the criteria.

Irrespective of the reporting format an audit function uses, these elements should generally be included in some form in each finding to address and report audit issues effectively. For root cause analysis, auditors need to drill down a little further on the last two components—consequence and corrective action plans/recommendations—to ensure they add value.

When noting a condition's business impact in an audit finding, one of four levels may apply:

- » Direct, one-time effect on the process.
- » Cumulative effect on the process.
- » Cumulative effect on the organization.
- » High-level, systemic effect.

In response to these levels, three important types of recommendations/action plans can be considered. The first two are described in the IIA Practice Guide, Audit Reports: Communicating Assurance Engagement Results":

- » Condition-based recommendations—provide an interim solution for correcting the current condition (e.g., removing inappropriate access).
- » Cause-based recommendations—actions needed to prevent the condition/observation from occurring again. Root cause-based recommendations are typically longer term solutions and may involve more time (e.g., creating and implementing an access review policy).

A third type of recommendation/action plan must be considered when the root cause has created a consequence whose damaging effects must be remediated before business continues:

- » Recovery-focused—address the consequences of the condition and describe what will be done to correct errors caused by it.

As illustrated by disasters such as the Deepwater Horizon oil drilling accident, which resulted in 11 deaths and caused the largest oil spill in U.S. history, identifying the root cause to prevent such a catastrophe from recurring is only one

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

part of the solution—someone also has to clean up the oil. So, in addition to a recovery-focused root cause analysis effort to get to the root cause of the spill's consequences, a recovery-focused recommendation and action plan would be needed to address the environmental damage.

Internal auditors should consider that the level of the effect will drive the nature of the root cause analysis and the type of recommendation and action plan:

- » Direct, one-time effect on the process (condition-based recommendation and action plan).
- » Cumulative effect on the process (cause-based recommendation and action plan).
- » Cumulative effect on the organization (recovery-focused recommendation and action plan).
- » High-level, systemic effect (recovery-focused recommendation and action plan).

As noted in Audit Reports: Communicating Assurance Engagement Results, "Action plans are effective when designed and executed in a way that addresses the root cause." In that regard, root-cause analysis has the aim of generating and formulating agreed-upon corrective actions to eliminate, or at least mitigate, those causes to produce significant long-term performance improvement in addition to promoting the achievement of better consequences.

REAP THE BENEFITS

The resources spent on root cause analysis should be commensurate with the impact of the issue or potential future issues and risks. Before starting root-cause analysis for more complex issues, internal auditors should bear in mind that additional time may be required to analyze the processes, personnel, technology, and data necessary to generate agreed-upon corrective action plans that eliminate, or at least significantly mitigate, the root causes. An effective action plan brings the condition in line with the criteria and addresses the potential or existing harmful outcomes stated in the effect. In the end, this approach will allow the auditor, audit client, and organization to reap the full benefits that a well-executed root-cause analysis effort can provide. Ia

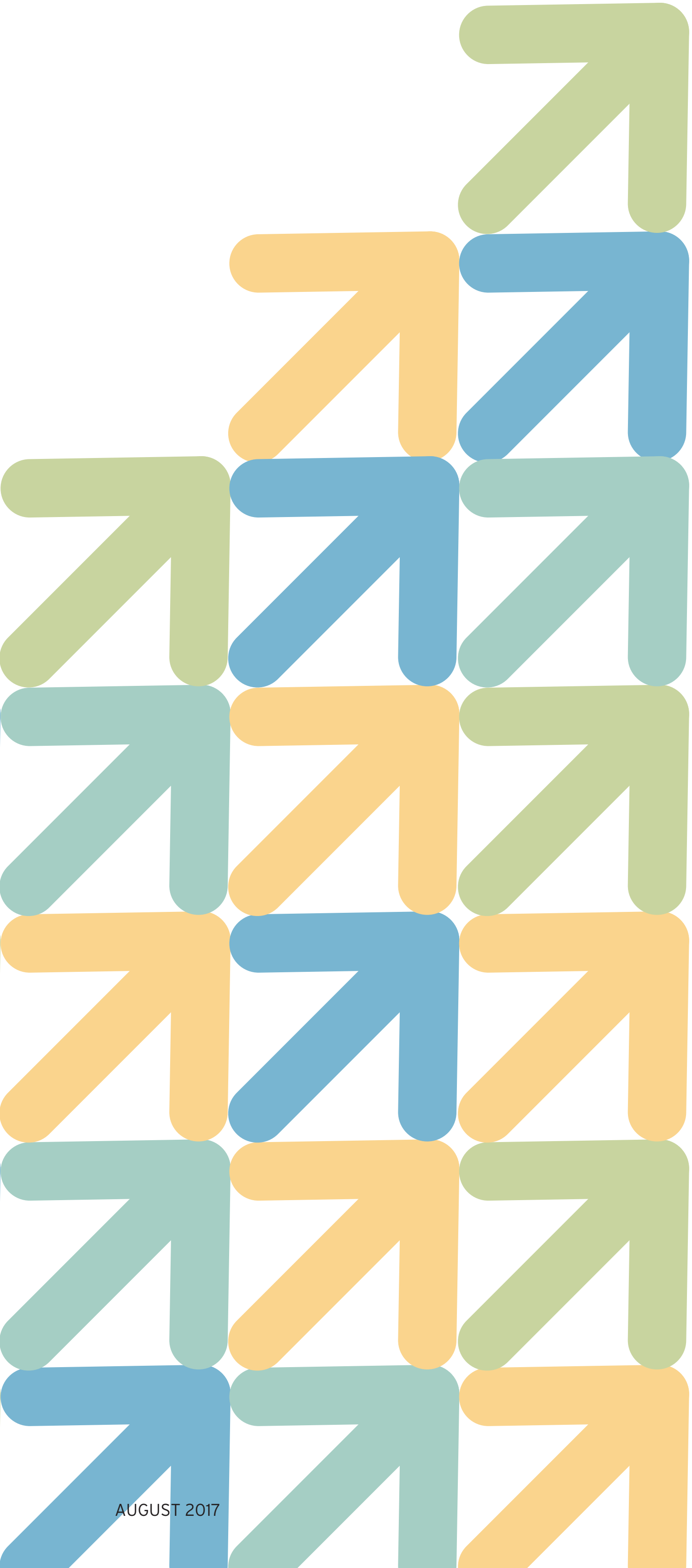
---

JIMMY PARKER, CPA, CIA, *is senior manager, internal audit, at Verizon in Lake Mary, Fla., and instructor for the IIA seminar, "Root-cause Analysis for Internal Auditors" (see "Calendar" on page 71).*

7 *Steps to Transformation*

Internal auditors can assist management throughout the many stages of business change.

James E. Schulien



Globalization, disruption, innovation, and continually evolving technology are driving a wave of business transformations. Such transformations involve making fundamental changes to how business is conducted to help cope with a shifting market environment, gain a competitive advantage, or reinvent the organization. These changes are frequently facilitated by implementing or upgrading IT systems such as core business applications.

Yet according to consulting firm McKinsey, 70 percent of business transformations fail. Many efforts to understand this result have focused on failures in change management and establishing a vision. Although these are critical elements in any business transformation, there are many common pitfalls that can derail these initiatives, including failing to manage change and communicate management's vision. These pitfalls are process, project, and control risks that fall squarely within the core competencies of the internal auditors. By inserting itself at seven steps of the transformation process and addressing these risks, internal audit can assist management in beating the odds and achieving a successful transformation.

1. PRE-IMPLEMENTATION REVIEWS

A pre-implementation review can help management identify problems in the planning stage—before they develop into costly missteps. An ideal pre-implementation project asks the question: What is the best practice model that should be applied to this transformation or new system implementation?

Pre-implementation projects identify the gaps between the best practice approach and the current planned approach for the transformation. For example, an aerospace manufacturer and integrator had processes and systems that were several generations behind the current state of the art. The company sought to modernize them by implementing the latest enterprise resource planning (ERP) suite and changing its processes to take advantage of the efficiencies the software provided. The company's internal audit function began a pre-implementation review by asking, what is the best practice project model for the implementation of complex ERP packages? The answer was a model that assessed project management risk, stakeholder commitment, functional risks such as defining requirements, change management risk, resource risk, and technical risks such as the IT controls testing methodology. This pre-implementation review identified issues with business owner approvals of process designs and acceptance of the benefits realization plan, the aggressive project timetable, and planning for regulatory compliance. Identifying these issues early allowed management to address them during the project.

"Top Transformation Pitfalls" on page 63 summarizes the most common transformation process, project, and control risks, and describes how internal audit can address these risks through pre-implementation reviews and other projects.

2. PROCESS/CONTROLS ANALYSIS

During a business transformation, it is easy for the project leaders to focus solely on the steps required to make a new application function appropriately. The real key to success with new systems is to take maximum advantage of the tools provided by the software to make the organization's processes more effective in meeting business objectives.

Leveraging the power of the latest software and achieving the transformation's goals come from an equal focus on both system functionality and processes and controls. This is an area where internal audit can advise process owners on how to structure processes and controls to take advantage of the new application and make the organization's new controls efficient.

In some transformations, auditors provide this process and controls advisory assistance directly to the project team. In other transformations, internal audit becomes a controls team champion. Ideally, the organization and staffing for a major business transformation will include a controls team. The controls team works full time as part of the project team to assist process owners in reengineering their processes and controls to fit the new business structure.

Ideally, a major business transformation will include a controls team.

3. IN-FLIGHT REVIEWS

One of the biggest challenges in a large transformation or system implementation effort is getting accurate data on the progress of systems development work and the quality of the modules being produced. Sometimes, project team members are reluctant to admit when objectives are not being achieved and communicate this bad news up the chain of command. As a result, project teams and project managers frequently report that a transformation project is on track when, in fact, it is far behind schedule. Moreover, the Ethics & Compliance Initiative's 2016 Global Business Ethics Survey of more than 13,000 employees notes that pressure to compromise standards and observed misconduct are most common in organizations undergoing change.

Internal audit reviews performed during the transformation project, rather than at the beginning or end, can assist management in assessing whether a project is on track to achieve its objectives. These in-flight reviews can address the same areas as the pre-implementation review, such as project management risk, stakeholder commitment, and functional risks. It also can concentrate on specific areas of concern such as whether the project is on track to achieve a specific goal.

4. IT AND USER ACCEPTANCE TESTING

When projects fall behind, leaders naturally look for ways to get the project back on schedule. Shortening the IT and user acceptance testing cycle is one method used to make up time. Although taking systems and user acceptance testing shortcuts may create the illusion of saving time, cutting corners almost always results in additional challenges that further delay the project. This produces the classic paradigm: "We did not have time to do it right the first time, so we ended up having to redo the effort."

Internal audit can contribute to IT and user acceptance testing by assessing the project's overall compliance with the company's full set of system development life cycle policies, or by assessing just the IT or testing processes. Auditors also can assist in user acceptance testing by advising process owners on testing methodology or by assisting in performing the testing in certain situations.

5. OUTPUT/RESULTS TESTING

Once the new processes and system are live and producing information for management's use, the output should be tested. While user acceptance testing is usually performed at the individual process level, testing of higher-level management accounting and operational

41% of business leaders surveyed say digital transformation has increased their organization's market share, according to Altimeter's 2016 State of Digital Transformation survey.

TOP TRANSFORMATION PITFALLS

A pre-implementation review can help management identify and prevent the 10 most common transformation pitfalls. Internal audit also can address risks at one of the other steps of transformation projects. The table below indicates how internal audit can address each risk.

	Risk	How Internal Audit Can Address the Risk
1	**Losing focus on the benefits to be achieved.**	Address in the project management risk phase of a pre-implementation review and during in-flight reviews.
2	**Failing to plan from beginning to end, and not including milestone goals and stages for the business.**	Address in the project management, requirements definition, and legacy system integration phases of a pre-implementation review, and during in-flight reviews.
3	**Insufficient investment in communications and change management.**	Address in the change management risk phase of a pre-implementation review and during in-flight reviews.
4	**Not anticipating challenges and road blocks. Building a plan that has no room for problems.**	Address in the project management risk and resource risk phases of a pre-implementation review, and during in-flight reviews.
5	**Failing to focus on processes and controls.**	Address in the requirements definition and legacy system integration phases of a pre-implementation review, and during process and controls advisory analysis and assistance.
6	**Taking system development life cycle shortcuts resulting in deployment of flawed software.**	Address in the IT controls testing methodology phase of a pre-implementation review and during IT and user acceptance testing assessments.
7	**Failing to begin with a pilot project, such as a test location or business unit, or proceeding before having success with a pilot.**	Address in the project management risk, legacy system integration, and stakeholder commitment phases of a pre-implementation review, and during in-flight reviews.
8	**Retiring a legacy system too soon, and failing to run the legacy system in parallel with the new system.**	Address in the legacy system integration and IT controls testing methodology phases of a pre-implementation review, and during IT and user acceptance testing.
9	**Failing to monitor progress and assess whether the project is still on track to achieve the benefits of the investments. Failing to obtain accurate information on progress.**	Address in the change management and project management risk phases of a pre-implementation review, during in-flight reviews, and during output/results testing reviews.
10	**Not celebrating successes throughout the project, and not rewarding and encouraging the project's champions.**	Address in the change management phase of a pre-implementation review and during in-flight reviews.

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

reporting output is needed to ensure this information is reliable. At this stage, internal audit can provide assurance that the new system produces accurate management information on operations, production status, costs, and profit.

Likewise, financial reporting information must be reliable. Testing financial reporting information produced by the new system is a critical part of the organization's assessment of internal control over financial reporting before the new system goes live. Internal audit should assess how the new processes and system will impact the design of internal controls of financial reporting and determine whether appropriate control design changes are being made as part of the transformation.

The high level of risk is why internal audit should participate.

6. POST-IMPLEMENTATION REVIEWS

For nearly all new system implementations, there is a time after the new system goes live when there is a high level of system change and correction requests. Post-implementation reviews can help management understand and prioritize corrections and changes to best align the corrective actions with the project's objectives. Ideally, a post-implementation review would be scoped to assist management in understanding how well the planned objectives have been met.

Post-implementation reviews also can help management understand what process and control issues remain to be addressed. Not all of these issues can be anticipated. Addressing the issues that are identified once the system comes online is another critical element in achieving the benefits originally sought when the transformation project began. As with designing good processes and controls into the project, addressing the control issues that develop later in the transformation life cycle can help prevent operational challenges and financial reporting issues from appearing after the organization has begun relying on the new processes and system.

7. COMPARISON TO PROJECT MANAGEMENT REVIEWS

In some respects, transformation projects are like any other project management review. Internal auditors are assessing whether the project is achieving the objectives that were the basis for its approval by management. The difference is that business transformations, by their very nature, are larger in scope and complexity than individual capital projects or investment initiatives.

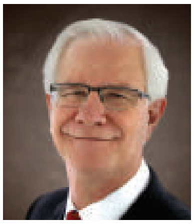
Transformations involve most, if not all, of the key management and board stakeholders in a business, and cross many functional and operational lines. Frequently, the future success of the business depends on the success of the transformation. This high level of risk to the business is the reason that internal audit should actively participate in its organization's business transformation initiatives.

ORGANIZATION TRANSFORMED

Achieving success with a large transformation is a daunting challenge for management. Internal audit's involvement can help management avoid the most common pitfalls and provide advice for building processes and controls that allow the organization to realize the benefits of its investment. In turn, these efforts can transform internal audit's reputation as a business partner and strategic contributor. Ia

JAMES E. SCHULIEN, CIA, CPA, *is president of Schulien Advisory Services in Fort Worth, Texas.*

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



BY J. MICHAEL JACKA

IT'S ONLY ONE WORD

Excessive audit report wordsmithing is often a disservice to the client—and the audit function.

It's so easy to change a single word … and so easy for that simple change to impact a sentence, a paragraph, or an idea. Rock musician Warren Zevon wrote an amazing song titled "Carmelita," which includes the line, "I pawned my Smith Corona. …" For those who don't know, a Smith Corona is a typewriter: a tool that, before the proliferation of computing power, was widely used by writers everywhere—even internal auditors. In that simple phrase, Zevon describes a man who has reached the end of his rope, pawning a valuable tool of his trade.

American pop singer Linda Ronstadt, in a typically incredible performance, covered the song. However, she made a small but significant change—"I pawned my Smith & Wesson. …" Again, for those who don't know, Smith & Wesson is a brand of firearms. Ronstadt's alteration seems minor, yet it changes everything about the lyric, its impact, and the story told by the song. It significantly modifies what was originally written.

And it is with no less impact that some reviewers make changes to audit reports, far too often altering those reports without ensuring that the change is necessary or appropriate. Words are precise, and when audit management assigns auditors to write those reports, management should expect the auditors to use the precise words that mean precisely what they mean to say.

Yet many audit report review processes seem designed to take away the auditor's responsibility for that precision. Far too often, the lead, manager, chief audit executive, etc. doesn't like what is written ("I can't say why; I just don't like it") and starts editing. The process often results in a report the auditor no longer recognizes and, in the worst situations, it says something the auditor never intended it to say.

Report reviewers everywhere, here are three lessons you should take to heart:

- Do not change anything without ensuring those who actually did the work have a say in those changes. That is the only way to ensure the report is still accurate.
- Never make a change unless you can explain why that change is necessary. Otherwise, you are just changing for personal preference.
- Always explain the reasons for any change to the person who wrote the original drafts. Only by understanding the reason for the changes will that individual ever learn how to do a better job.

However, there is a fourth and just as important lesson that seems counterintuitive in a discussion about the preciseness of words. Don't dither.

Internal auditors work hard to find the exact wording when something close will do. And our focus on that unnecessary precision results in a deluge of rewrites, delays, and frustrations. Get it right, but don't worry about being perfect. And when all is said and done, make sure you haven't turned a typewriter into a gun. Ia

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

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

THE DATA ANALYTICS STRATEGY

Adding analytics to the audit methodology requires careful change management.

STEFAN DAVIS
Product Owner,
TeamMate Analytics
Wolters Kluwer

SERGIU CERNAUTAN, CPA, CISA
Director, GRC Strategy
ACL

What are the key components of an effective data analytics strategy?

CERNAUTAN Successful data analytics strategies should start by building an internal business case, as these programs often lose momentum and fail if their value is not appropriately "sold" within the organization. Next, address the knowledge and skill gaps by allocating funding to resource and train the audit teams. When it comes time to buy, invest in modern technologies that are easy to use and implement. For maximum impact, integrate data analytics requirements into the audit methodology. Make the use of analytics required rather than optional. Aim for quick wins that will naturally progress to larger successes by phasing the program in with an agile methodology. By focusing on automating routine audit areas, teams can self-fund the program through efficiency gains and demonstrated return on investment.

DAVIS The key component for developing an effective data analytics strategy involves changing the way you think about your work. Start with defining the objectives you are trying to achieve either for your audit team or your audit cycle. Then plan and execute a vision for using data analytics to achieve your objectives. You'll need strong support from senior management and buy-in from the audit staff to gain efficiencies in meeting your objectives. Tools that are easy to use, train on, and deploy will lead to quick wins and help with buy-in and boost the data analytics strategy momentum for more advanced analytical strategies down the road. An analytics lead or champion should be responsible for executing the strategy. To track progress, set targets and monitor key performance indicators such as the percentage of audits performing at least one analytics test.

What do CAEs need to know before jumping in?

DAVIS Changing from traditional audit techniques to incorporating analytics is not always an easy exercise. Including analytics is a significant change in methodology, especially for experienced auditors, and it requires careful change management. The chief audit executive (CAE) needs to set expectations for the analytics effort, making it clear to the auditors that analytics is a priority for the department to gain efficiencies in meeting audit and department objectives. Knowing when to apply analytics and identifying opportunities for efficiency gains with analytics are critical to implementing a strategy.

CERNAUTAN Over the past 20 years, the CAEs I've worked with who struggle to implement a successful analytics program all cite at least

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

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

one of three factors: 1) difficulty in accessing data; 2) lack of data analytics skills; and 3) the high costs to implement. This may have been true years ago, but in today's world it is simply not the case: Data is easier to access; analytic tools are powerful, flexible, and easy to use; and the cost of not implementing vastly outweighs the cost to implement. To remain relevant, internal audit must adopt analytics literacy as a basic requirement. In today's world of big data, social media, and increasing risk velocity, it is impossible to fulfill the internal audit mandates of "adding value and improving an organization's operations" and "improving the effectiveness of risk management, control, and governance processes" using antiquated manual audit processes that focus solely on post-detection techniques.

How can data analytics be leveraged to strengthen risk assessments and the audit plan?

CERNAUTAN The greatest risk is the unknown. Integrating analytics into risk assessments confirms the completeness of identified risks, and assumptions made about them, while illuminating potential gaps. By applying data analytics to support your risk assessments, the resulting audit plans will be better informed and developed from objective measures rather than subjective ones, which are prone to error. Forrester analyst Nick Hayes puts it this way: "Your assumptions about risk are deeply flawed without analysis of actual transactional data."

DAVIS In the past, analytics have been primarily focused on fieldwork, but they can add huge value to risk assessment and planning. In audit planning, data analytics allow audit departments to gather company, industry, and prior audit results to help drive the audit plan. Visualization and summarization, along with regression and trend analysis, can highlight changing and emerging risks as well as issues to target and explain current and future audit coverage.

How can data analytics be leveraged to strengthen individual audit engagements?

DAVIS Starting with engagement planning, auditors should consider opportunities to incorporate data analytics. If an audit is repeated, revisit audit programs to see where analytics will add value, rather than repeating manual tests. Getting data relevant to the audit objectives before fieldwork begins will allow preliminary analytics to identify risks that may influence audit scope. In fieldwork, data analytics will strengthen an audit through the ability to analyze complete data sets, rather than sampling. Complete testing leads to deeper insights into processes and procedures. Testing every instance of a control provides more robust audit evidence and increased coverage provides greater assurance. When reporting issues, deeper insights can be supported by tangible, measurable valuations. Rather than saying "we tested 30 purchases and found two without authorized purchase orders," analytics allows you to say "we tested the full population of purchasing transactions, and found $84,234 in purchases with unauthorized purchase orders." When they can see the dollars involved, management has a reason to follow or correct a control.

CERNAUTAN One cannot truly achieve a risk-based audit approach and add value without being data driven throughout. From the initial risk assessment, to scoping and planning, to executing fieldwork, to raising issues, and all the way to preparing the final audit report—the nature, timing, and extent of procedures to be performed are largely driven by the magnitude of the risks. What better way to quantify the risks, rationalize your audit effort, and support your results with evidence than by analyzing actual data?

What's more, executives constantly ask "so what?" to challenge the value of audit findings. Transform that response by supporting findings with objectively quantifiable data and key performance metrics. Consider a process recommendation to "take advantage of procurement discounts by accelerating net payment terms," subjectively rated as high impact. Consider the same recommendation, objectively supported by data. "If we had taken advantage of the procurement discounts offered over the last year, we could have avoided $10 million in costs." Which is more compelling and relevant to the organization?

How can auditors use data visualization to communicate audit results?

CERNAUTAN To be effective, visualizations must be social, interactive, and actionable. In an increasingly technological and social world, auditors can communicate visualizations more effectively using social media tools such as virtual storyboards. Incorporating elements of interaction further increases stakeholder engagement by allowing recipients to pull relevant information and trigger responses or actions based on what they see.

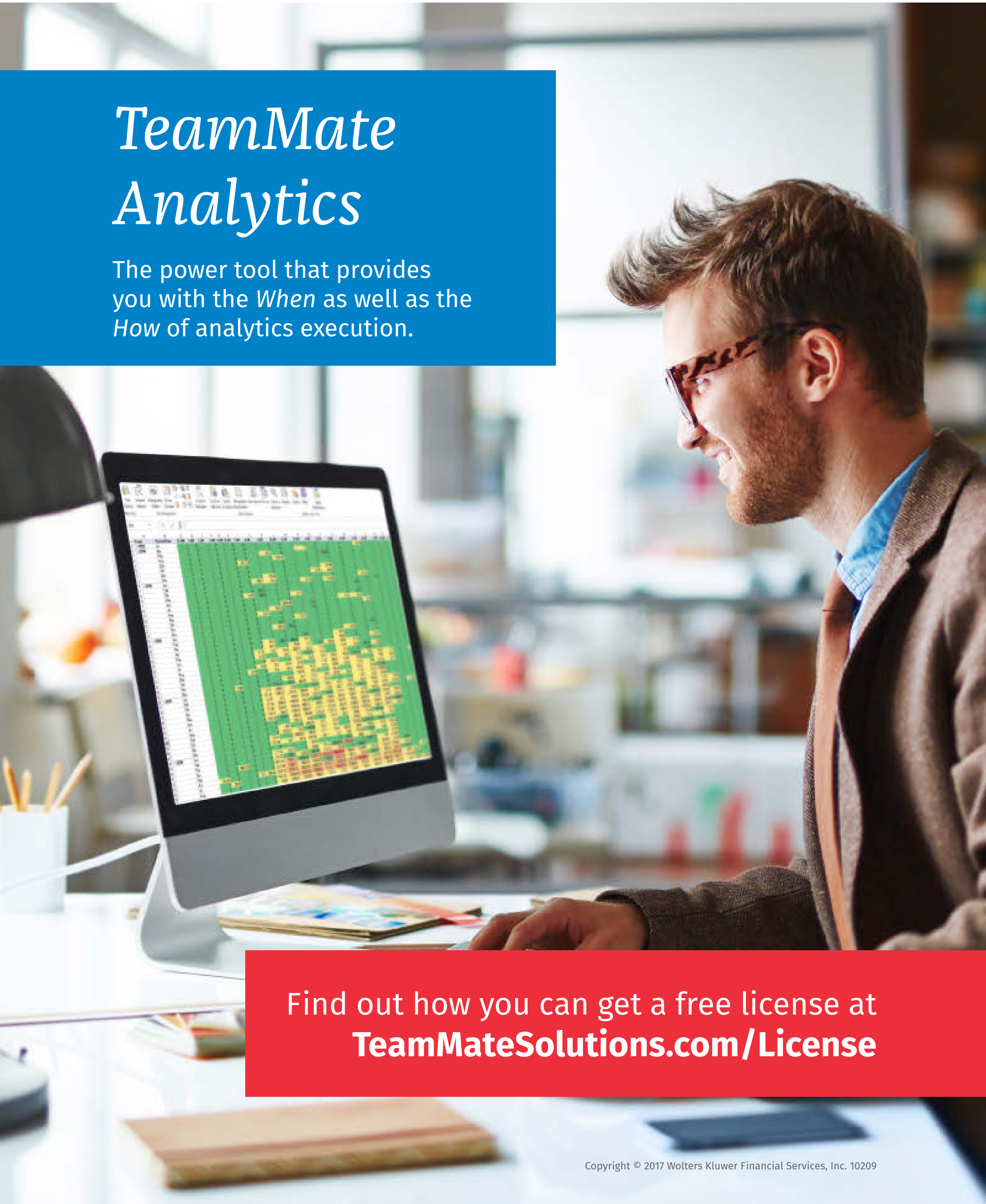
DAVIS Presenting data visually makes it easier to digest. You need to start with the message that you are trying to communicate, which in the case of audit results can be complex. Through the use of visualization, you can communicate a single message and answer detailed questions in a single image. For example, you can show the highest risk category over the last year by location from one visual as opposed to reviewing pages of detail. Visualizations do not need to be complicated. The key is to keep it simple with line charts showing trends over time and bar charts for non-time-based information. Ia

Wolters Kluwer

When you have to be right

TeamMate Analytics

The power tool that provides you with the *When* as well as the *How* of analytics execution.



Find out how you can get a free license at
TeamMateSolutions.com/License

IIA Calendar

PHOTO: RAWPIXEL.COM / SHUTTERSTOCK.COM

IIA CONFERENCES
www.theiia.org/conferences

AUG. 16–18
Governance, Risk, and Control Conference
Gaylord Texan
Dallas-Fort Worth

SEPT. 11–12
Environmental, Health & Safety Exchange
Hyatt Regency St. Louis
St. Louis

SEPT. 18–19
Financial Services Exchange
Renaissance Downtown Hotel
Washington, D.C.

SEPT. 18–20
Southern Regional Conference
Hilton Austin
Austin, TX

OCT. 29–NOV. 1
All Star Conference
Bellagio Hotel
Las Vegas

IIA TRAINING
www.theiia.org/training

AUG. 7–9
Auditor-in-charge Tools and Techniques
Data Analysis and Sampling
Cleveland

AUG. 8–11
Various Courses
Chicago

AUG. 15–17
Auditor-in-charge Tools and Techniques
Beginning Auditor Tools and Techniques
Seattle

AUG. 15–24
Assessing Risk: Ensuring Internal Audit's Value
Online

AUG. 21–30
Performing an Effective Quality Assessment
Online

AUG. 22–25
Various Courses
Dallas

AUG. 28–31
Various Courses
Palm Beach, FL

AUG. 29–30
Root-cause Analysis
(pilot course, discounts available)
Lake Mary, FL

SEPT. 5–14
Cybersecurity: Auditing in an Unsecure World
Online

SEPT. 6–15
Risk-based Auditing: A Value Add Proposition
Online

SEPT. 10, 13–14
Various Courses
St. Louis

SEPT. 11–13
Vision University
San Diego

SEPT. 11–20
ERM: Elements of the Process
Online

SEPT. 12–15
Various Courses
New York

SEPT. 19–20
Data Analysis for Internal Auditors
Online

SEPT. 19–22
Various Courses
Boston

SEPT. 21
Fundamentals of Internal Auditing
Online

SEPT. 25–28
Statistical Sampling for Internal Auditors
Online

OCT. 2–11
Fundamentals of IT Auditing
Online

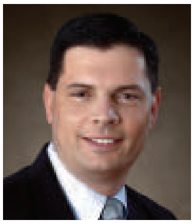
OCT. 2–18
CIA Learning System Comprehensive Instructor-led Course; Part 2
Online

OCT. 3–12
Lean Six Sigma Tools for Internal Audit Fieldwork
Online

OCT. 23–27
Various Courses
San Diego

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

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



BY JIM PELLETIER

FROM RATINGS TO RECOMMENDATIONS

Behavioral psychology suggests internal auditors' approach could benefit from more carrot and less stick.

Audit ratings may be the most misused tool in the auditor's tool belt. Instead of motivating management to fix problems, ratings more often serve as a demotivator, answering the question, "How bad is it?" This is the wrong question, and it erroneously imposes a "stick" mentality. While ratings may get the attention auditors are looking for, they undermine any attempt to build strong, professional relationships and fail to encourage constructive behavior. If we believe in our mission as stated in The IIA's International Professional Practices Framework—"to enhance and protect organizational value"—then the goal of any audit is not to demonstrate just how bad things are, but to encourage positive action in support of the organization's goals.

Many internal auditors report long lists of open audit recommendations and management's resistance to implementing them, ranging from passive-aggressiveness (ignoring the recommendations) to outright denial that any problems exist. Auditors will say that it's not personal, that they are just doing their job. They often think the client should be mature enough to not take being audited personally. But when you are the subject of an audit that could potentially expose your weaknesses all the way up through the C-suite to the board, it's unavoidably personal. Add to that the audit ratings—essentially bright flashing arrows pointing out problems—and you have the makings of a difficult relationship with management. How can auditors transform this stick into a carrot? To begin, it helps to understand a few basics on motivation.

What truly motivates people has been studied for years by University of Rochester researchers Edward Deci and Richard Ryan. Their research has culminated in what they call the self-determination theory (SDT), which posits that human motivation is optimized when three basic needs are met: developing one's skills (competency), exercising free will (autonomy), and feeling connected with others (relatedness). According to SDT, motivation through common meaningful goals will trump negative reinforcement every time. The researchers also found that while negative reinforcement can be effective, the impact is often temporary and can incentivize undesirable behavior.

Instead of rating audit findings, internal auditors should prioritize recommendations. In other words, don't focus on what is wrong—bring attention to the most important actions required to manage risks. The chief audit executive for the County of Los Angeles, Peter Hughes, explained at the recent IIA Western Regional Conference that he uses this strategy to great effect. Brilliant in its simplicity, the approach is future focused on solutions rather than looking backward at past mistakes. Most importantly, as SDT points out, by focusing on developing common goals via prioritized recommendations, management will be far more motivated to take ownership. Instead of grading their level of incompetence, give them the opportunity to implement solutions and demonstrate their competence, autonomy, and relatedness. Ia

JIM PELLETIER, CIA, CGAP, *is vice president, Professional Solutions, at The IIA.*

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