JUNE 2020

A PUBLICATION OF THE IIA

Ia INTERNAL AUDITOR

Questions the Audit Committee Should Ask

Protecting Privacy in a Volatile World

IIA's New N.A. Board Chair on Building Great Teams

Audit's Value Proposition: 2.0

ROAD TO RECOVERY

In the age of COVID-19, internal auditors can help organizations navigate immediate risks, while keeping an eye on the horizon.

Ia
INTERNAL AUDITOR

JUNE 2020 VOLUME LXXVII: III

FEATURES

Ia
INTERNAL AUDITOR

JUNE 2020 VOLUME LXXVII: III

DEPARTMENTS

PRACTICES

INSIGHTS

ONLINE InternalAuditor.org

The Virtual Audit Whether working from home or an office, managing remote audits requires attention to logistics and consideration of stakeholder needs.

Testing the Boundaries Although some regulators are easing rules to help businesses through the pandemic, legal experts warn companies against pushing the limits of what's allowable.

The Analytics Development Process A consistent approach facilitates communication and the chances of consistent results in the latest chapter of The Analytics Journey.

Police Entangled in Tow-truck Kickbacks Law enforcement agencies need strong ethics policies and procedures to deter officers from cashing in on corruption.

Find us on Facebook

COVER: SKY, BLUEBEAT76 / ISTOCK.COM; ROAD, ROST-9D / ISTOCK.COM; THIS PAGE, TOP: NOMAD_SOUL / SHUTTERSTOCK.COM, BOTTOM: ANDRII YALANSKYI / SHUTTERSTOCK.COM

Internal Auditor ISSN 0020-5745 is published in February, April, June, August, October, and December. Yearly subscription rates: $75 in the United States and Canada, and $99 outside North America. No refunds on cancellations. Editorial and advertising office: 1035 Greenwood Blvd., Suite 401, Lake Mary, FL, 32746, U.S.A. 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.

President's Message

EVOLVING TO MEET YOUR NEEDS

From its first issue in 1944, *Internal Auditor* magazine has chronicled the advances, the challenges, and the evolution of internal auditing. Through these pages, we have witnessed the profession rise from a focus almost exclusively on financial matters to its establishment as a major force in governance and crucial to organizational success.

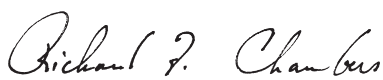
More than ever, *Internal Auditor* readers are hungry for information when and where they need it most. That shows in increased readership of magazine and online-exclusive content on InternalAuditor.org, launched in 2008. In fact, since the coronavirus was designated a pandemic by the World Health Organization, visits to the magazine's website have surged 13%.

In response to reader expectations, the magazine is focusing its energy and resources where they are of most value to you—on developing and delivering timely and relevant content. To do that, we will be suspending the print edition after this issue. This is a natural progression, one that we have been examining for a long time, as readership habits turned to more on-demand interests. For those of you who have grown comfortable receiving the magazine in print form, that format will continue to be available for online viewing or through download. In addition, your subscription will not be affected, as it remains an important benefit of membership in The IIA.

Rest assured, *Internal Auditor*'s highly experienced team of editors and writers will continue to work tirelessly to keep you, the magazine's readers, up to date on the latest developments, especially those around COVID-19 and how they are impacting internal auditing. In this issue, for example, the magazine features several articles related to COVID-19, providing valuable information to practitioners who are moving forward during these difficult times.

The cover story, "Navigating the Crisis" (page 22), considers how internal auditors can help management address short-term risks while keeping an eye on what lies farther down the road. You'll also want to read *Internal Auditor*'s online exclusives, including "Responding to the Crisis," a look at The IIA's approach to business continuity. Also on InternalAuditor.org, the editorial team has started a COVID-19 Newswire, with daily updates as organizations turn to the next phase of the crisis.

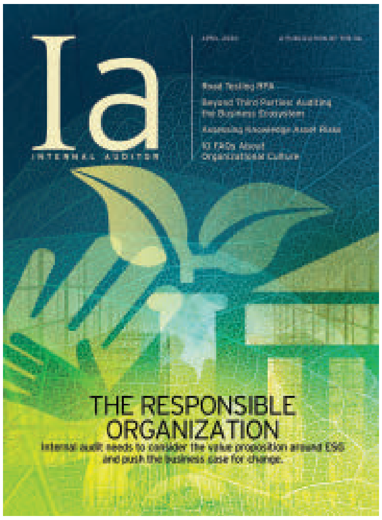
Our commitment to members and subscribers has never wavered. We pledge to work toward providing indispensable information to professionals who want to keep pace with the diverse, dynamic field of internal auditing. And we look forward to you joining us online to see what's coming over the horizon.



Richard F. Chambers, CIA, QIAL, CGAP, CCSA, CRMA
President and Chief Executive Officer
The Institute of Internal Auditors

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.



No Surprises

I really thought that Steve Mar's advice for the unexpected question from the audit committee (which always seems to come up) was smart: "Good strategic question. Let me gather hard data first before I answer you. If I need help to solve this, can I count on your support?"

One tactic that has been beneficial to me is running a preparation session with other executives to try to anticipate the unexpected questions that might come up. Regardless, the golden rule of board discourse is: No surprises. I think Mar captured that well.

CHRIS DENVER *comments on Steve Mar's "My First Audit Committee Meeting" (InternalAuditor.org).*

Embrace the Experience

When I came back from paternity leave, I began working from home. I'm also homeschooling two of our children. Having a routine, always growing, and looking for ways to add more than to take are helping me. Also, keeping in mind that this crisis is only temporary—when will it end, who knows?

But, going back to Richard's first point, embracing the experience—looking for the blessing rather than the discomfort—definitely helps a lot.

EZEKIEL ABENDAN *comments on the Chambers on the Profession blog post, "Are You Sheltering at Home in Color?" (InternalAuditor.org).*

Definition of Risk

Mike Jacka makes an excellent point that the word *risk* is not commonly understood. Unfortunately, his definition of *risk* is not the one used in the global standard.

Risk is not an event, it's the effects of an event or situation on objectives. The fact that people don't have the same understanding of this four-letter word should help us see that it is better not to use it.

Let's replace that four-letter word, and its negative connotations, with "what might happen." Then, perhaps, people will see that we should be focusing less on avoiding or mitigating the bad stuff and instead focusing on what we need to do (including taking risk) to be successful.

NORMAN MARKS *comments on the From the Mind of Jacka blog post, "Risk and Uncertainty" (InternalAuditor.org).*

After the Crisis

One thing I'm learning in the current crisis is that all weaknesses and strengths of an organization are being exposed. As auditors, we are seeing first-hand the challenges we will be facing going forward. Thanks for the post as it really hit home right now.

DAN MCPHERRON *comments on the From the Mind of Jacka blog post, "The Divot of Complacency" on LinkedIn.*

Ia
INTERNAL AUDITOR
JUNE 2020
VOLUME LXXVII:III

EDITOR IN CHIEF
Anne Millage

MANAGING EDITOR
David Salierno

ASSOCIATE MANAGING EDITOR
Tim McCollum

SENIOR EDITOR
Shannon Steffee

ART DIRECTION
Carol Hardy Design

PRODUCTION MANAGER
Gretchen Gorfine

PUBLISHED BY THE INSTITUTE OF INTERNAL AUDITORS INC.

CONTACT INFORMATION

ADVERTISING
sales@theiia.org
+1-407-937-1388; fax +1-407-937-1101

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

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

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

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

Stakeholders watching complex risks... Budget woes may cut fraud defense... Switching vendors in a crisis... Bad environmental practices could hurt credit.

Update

CYBERCRIME'S BOTTOM LINE

A survey of U.S. IT security professionals shows the average total cost of a cyberattack across several categories.

$1.5 MILLION Nation-state

$1.2 MILLION Zero-day

$832,500 Phishing

$691,500 Spyware

$440,750 Ransomware

Source: Ponemon Institute and Deep Instinct, The Economic Value of Prevention in the Cybersecurity Lifecycle

RECOVERY THROUGH DIGITIZATION

Research points to technology as a key driver for crisis navigation.

A new report from McKinsey & Co. advises businesses to focus on digitization as a means of navigating the coronavirus pandemic. Flexibility and speed will be key as organizational leaders consider how to move ahead, the consulting firm says in The Digital-led Recovery From COVID-19: Five Questions for CEOs, which draws on observed best practices.

With COVID-19 putting outdated business models to the test, the shift to digital will likely accelerate. Organizations need to take bold action, the report advises, tempered with "a full appreciation of risk from the impact of cyberattacks to the loss of crucial talent." Incremental technological change and half measures are recipes for failure, the report's authors say.

Making the right technology investments will be crucial moving forward, requiring organizational leaders to work closely with their technology officers to update legacy systems and establish new digital capabilities, McKinsey notes. Technology is a key driver of value—and that includes the use of advanced analytics.

"Never before has the need for accurate and timely data been greater," the report says. At the same time, CEOs will need to work with their risk leaders to make sure the

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

IMAGES: TOP, LEIGH PRATHER / SHUTTERSTOCK.COM; LEFT, NOMAD_SOUL / SHUTTERSTOCK.COM scramble to harness data follows strict privacy rules and cybersecurity best practice.

To ensure technology initiatives materialize, CEOs also may need to have a long talk with their chief financial officers. PwC's COVID-19 CFO Pulse Survey shows that more than two-thirds of surveyed finance chiefs say they plan to defer or cancel planned investments in response to the crisis—and of those, more than half say they are eyeing IT initiatives for the chopping block. Another 25% say they are deferring or canceling digital transformation investments. **—D. SALIERNO**

GREATER RISK BRINGS NEW SCRUTINY

Stakeholders may find risk management processes lacking, report finds.

Today's riskier business environment is pressuring organizations to disclose more about risk management, according to the 2020 State of Risk Oversight. Nearly 60% of the 563 U.S.-based chief financial officers surveyed say risks are growing extensively in volume and complexity, particularly in areas such as talent, innovation, the economy, and brand.

With greater risk has come heightened attention, notes the report from the American Institute of Certified Public Accountants and North Carolina State University's ERM Initiative. Two-thirds say boards are calling for more management oversight of risk, while 58% say outside parties such as investors are demanding extensive detail about how organizations manage risk.

Yet, only one-fourth of respondents say their organization's risk management is mature, a decline from previous surveys.

Moreover, less than 20% say their risk management process provides strategic value. "If functioning effectively, a robust enterprise risk management process should be an important strategic tool for management," the report says. **—T. MCCOLLUM**

75%

OF U.S. ADULTS SAY THAT COMPANIES have a responsibility to support coronavirus relief.

71%

SAY THEY WILL STOP PURCHASING PRODUCTS from companies they perceive to be irresponsible during the crisis.

"Americans are watching which companies are stepping up at this time," says Kate Cusick, chief marketing officer at public relations advisory firm Porter Novelli/Cone. "The decisions businesses make today will define them well after this pandemic has passed."

Source: Porter Novelli/Cone, COVID-19 Tracker: Insights for a Time of Crisis

WEIGHING THE COST OF FRAUD

Fraud defenses work but could face the budget-cutting ax.

Organizations already pay a steep price for fraud, but they may be targeted even more if budget-cutting weakens defenses such as internal audit. Occupational fraud costs organizations about 5% of annual revenues, according to the Association of Certified Fraud Examiners' (ACFE's) 2020 Report to the Nations.

The report analyzed more than 2,500 fraud cases from 125 countries, with losses totaling more than $3.6 billion. Most of these frauds come from four areas: operations (15%), accounting (14%), executive management (12%), and sales (11%).

In a post previewing the latest report, ACFE President and CEO Bruce Dorris

IMAGES: TOP, YULIA SUTYAGINA / ISTOCK.COM; RIGHT, RETROROCKET / ISTOCK.COM

warns organizations not to cut internal audit and compliance amid the economic fallout from the coronavirus. "Cutbacks to departments or initiatives that are integral to a comprehensive anti-fraud program only serve to leave organizations more vulnerable to the growing likelihood of fraud," he says.

Weakened defenses combined with individuals facing financial pressures could create a "perfect storm" for fraud, Dorris cautions.

Effective controls, reporting, and training also help fraud fighting considerably, the report notes. One-third of frauds can be attributed to a lack of internal controls, so over the past decade, the use of controls such as hotlines, anti-fraud policies, and fraud training has increased by at least 9%. Organizations discover 43% of frauds through tips—half of them from employees—but employees are far more likely to report fraud when they receive fraud-awareness training.

One new trend the report finds is that individuals accused of fraud are less likely to face criminal charges, with organizations increasingly preferring to handle cases through internal discipline or civil litigation. Four out of five fraud perpetrators were disciplined internally, and 46% of victim organizations say they declined to refer cases to law enforcement because internal punishment was sufficient. **—T. MCCOLLUM**

SOURCING IN A CRISIS

New vendor relationships can create new risks, says Erich Heneke, director of business integrity and continuity at the Mayo Clinic.

COVID-19 has businesses looking at the viability of their vendors. How can businesses shift quickly to new vendors? The pandemic has not only exposed traditional vendor risks with respect to supply chain disruption, but it has unlocked a new set of brokered vendors that enter new risk into the market. In health care, products have become unavailable due to supply and demand issues through traditional channels, and, thus, we are seeking products in alternative markets. When sourcing alternate channels, we have seen an influx of counterfeit products as well as brokers requiring a pre-payment and then vanishing with the hospital's money, which suggests that new tools will be necessary to quickly vet new vendor relationships.

Internal audit should let business areas do what they do best, while providing higher and wider level views into enterprise risks. Auditors also should be available as consultants to help mitigate risks as they emerge in vendor markets, whether that's by helping to design a third-party risk management program or aid in strategic sourcing needs. Auditors can offer an independent set of eyes on a process that is largely unfamiliar to a health-care supply chain.

BROWN FACTORS MAY AFFECT CREDIT

Harmful activities may become targets of disincentives.

Organizations are familiar with "green" activities, but the environmentally harmful "brown" activities may have greater credit implications, according to Fitch Ratings' inaugural ESG Credit Quarterly report.

As defined by The European Commission's (EC's) final report on the European Union taxonomy for sustainable activities, green activities contribute substantially to environmental objectives. Since the report's publication in March, there have been calls for the commission to develop a taxonomy listing environmentally harmful (brown) activities.

The technical expert group assisting the EC with the sustainability taxonomy states that activities not defined as *green* should not automatically be considered *brown*. The Fitch report points out that consensus on a brown taxonomy will be difficult. However,

it could impact credit by defining targets for disincentive policies such as higher prudential capital requirements.

A brown taxonomy "could inform how asset managers and banks screen for other fossil fuels or environmentally harmful activities in the future," Fitch notes. Additionally, it could lead to greater standardization in how investors and banks screen sectors deemed harmful. **—S. STEFFEE**

PHOTO: RIGHT, IZNASHIH / ISTOCK.COM

Back to Basics

BY JONNIE KEITH EDITED BY JAMES ROTH + WADE CASSELS

WRITE EFFECTIVE AUDIT OBJECTIVES

Well-written objectives can define a successful internal audit.

Audit objectives are the mission statement, or the reason, for the audit engagement. Once they've been established, everything done on the engagement—either directly or indirectly—supports their achievement.

Audit objectives are one of the most important parts of the audit engagement, and they impact every aspect of it, including the:

- Audit scope, which determines how much evidence the auditors will review.
- Audit resources and how they will be deployed.
- Audit program that will be developed to achieve the audit objectives.
- Audit results, which reflect the achievement of the audit objectives.

Well-written objectives are crucial to performing an effective audit. There are three basic principles that can help develop effective audit objectives. Each objective should:

1. Be simple and focused.
2. Seek to reach a conclusion.
3. Be traceable to the summary results.

IIA *Standards* Relative to Audit Objectives

Based on the *International Standards for the Professional Practice of Internal Auditing*, the chief audit executive (CAE), in consultation with management, must develop a risk-based plan to determine the areas of significant risk to the organization. Those areas are then prioritized to ensure that audit resources are deployed accordingly. A preliminary assessment, with input from management, is conducted for each audit performed. Using the preliminary assessment results, the CAE then develops the audit objectives based on the selected risks, the available audit personnel, and the allotted time for the engagement.

Keep Objectives Simple and Focused

Each audit objective should be straightforward and not overly broad. It should be easy to identify what is to be accomplished. For example, the audit objective statement, "To determine that the preventive maintenance is done in accordance with policy and procedures," would imply that every control in the preventive maintenance process has to be tested. And the failure of any control, significant or not, would be subject to a write-up. It is better to focus on the top key controls for that area.

Now consider this example: "The objectives of the audit were to assess the weekly bus mileage reports to determine their accuracy and timeliness, to verify that preventive maintenance is performed timely, to confirm that mechanics received the requisite number of annual

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

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

AUDIT OBJECTIVE STANDARDS

Several IIA *Standards* relate to audit objectives, but the most significant are:

2010: Planning – "The chief audit executive must establish a risk-based plan to determine the priorities of the internal audit activity. ..."

2010.A1: Planning – "The input of senior management and the board must be considered in this [planning] process."

2200: Engagement Planning – "Internal auditors must develop and document a plan for each engagement, including the engagement's objectives. ..."

2210: Engagement Objectives – "Objectives must be established for each engagement."

2210.A1: Engagement Objectives (Assurance) – "Internal auditors must conduct a preliminary assessment of the risks relevant to the activity under review. Engagement objectives must reflect the results of this assessment."

2220: Engagement Scope – "The established scope must be sufficient to achieve the objectives of the engagement."

2230: Engagement Resource Allocation – "Internal auditors must determine appropriate and sufficient resources to achieve engagement objectives. ..."

training hours, and to evaluate whether repair parts were safeguarded adequately."

A simpler, clearer, and more focused audit objective statement would be: "The objectives of the audit were to determine whether:

- The weekly bus mileage reports were both accurate and timely.
- Preventive maintenance was performed timely.
- Mechanics received the requisite number of annual training hours.
- Repair parts were safeguarded adequately."

Using a bulleted list makes the audit objectives obvious and easy to follow. There is the added advantage that each bullet point can serve as an objective for developing a step-by-step audit program. Plus, the bullet points can be directly correlated to the summary results.

Seek to Reach a Conclusion

Each audit objective should try to reach a conclusion or seek to prove something. For example, the statement, "The objective of the audit was to assess the weekly bus mileage reports," does not constitute an audit objective. It states what is to be done, but it does not state what it is to accomplish.

Audit objective statements will generally have the words "to determine" or similar phrases such as "to assess," "to review," or "to evaluate." Audit objectives are essentially "yes or no" questions that seek some type of determination.

- Were the weekly mileage reports accurate and timely?
- Was preventive maintenance performed timely?
- Did the mechanics receive the requisite number of annual training hours?
- Were the repair parts adequately safeguarded?

Each objective should determine either "yes," the controls worked, or "no," they did not work or only partially worked.

Make Objectives Traceable to the Conclusion

The summary of findings should be worded very similar to, or mirror, the audit objectives. For example, the summary results statement would read:

"Based on the results of our review, analysis, evaluation, and testing, we determined that:

- The weekly mileage reports were accurate and timely.
- Preventive maintenance was performed timely except for… .
- Mechanics received the requisite number of annual training hours.
- Repair parts inventory was not adequately safeguarded."

Summary conclusions should be in the same order and read almost exactly like the audit objectives were written, making them easily traceable back to the audit objectives. The example shows that there were problems in the second and fourth conclusions.

The Value of Well-written Objectives

Because the primary mission of every audit engagement is to achieve the audit objectives, how well the objectives are written can be crucial to performing a successful audit. Applying the three principles when developing audit objectives will make them more effective and useful. It will ensure that audit objectives will be effectively addressed and audit resources can be more efficiently deployed. Ia

JONNIE KEITH, CIA, CFE, CGAP, *is an audit consultant with JonSherr Enterprise in Atlanta.*

BY JOHN VERVER EDITED BY STEVE MAR

EIGHT AREAS OF ANALYTICS ADVANCEMENTS

A survey shows internal audit functions are making progress in implementing data analytics.

Even internal auditors at a giant software firm like Microsoft have to get the basics right to make the most of data analytics. It takes a strategic plan, skilled resources, management support, and access to clients' data. "It took time and a sustained strategy to build up our data analytics muscle," says Pooja Sund, director of Technology and Analytics for internal audit at Microsoft.

Microsoft's experience is indicative of the significant progress many internal audit departments are making in implementing data analytics into their work, according to a new survey. The most advanced audit functions are applying suites of automated analytics across multiple business processes, performing sophisticated analytics, and using data from broad sources, notes The Audit Analytics Institute's (AAI's) 2020 Survey on the State of Data Analytics Usage in Internal Audit (see "Survey Highlights" on page 17). AAI polled audit executives, directors, managers, and analytics specialists from about 70 organizations for the report.

These departments have specialists to deal with the complex aspects of data analysis and formal procedures to ensure the quality and sustainability of analytics use.

Moving Beyond the Basics

Increasingly, internal audit functions are moving beyond basic uses of analytics, such as testing all general ledger transactions for suspicious journal entries or examining purchase and payment transactions for duplicates. One example of more advanced analytics is in a payroll audit in which auditors compare data from network logins and use of physical access swipe cards to payroll records to identify nonexistent employees or fraudulent overtime payments.

One survey finding calls out the strong correlation between teams that have deployed data analytics successfully and how they addressed implementation issues such as needing structures and processes. The survey findings yield takeaways across eight topic areas.

Strategy and Objectives

Six out of 10 audit teams have a clearly communicated audit analytics strategy, the survey finds. Nearly half have defined goals for analytics usage, and 68% of audit leaders are highly supportive of analytics. The takeaway for internal audit is that developing a formal, well-communicated audit analytics strategy, with specific goals and audit leadership's proactive support, is critical. For example, the strategy could be that for every audit, the department will evaluate the potential use of analytics, with a goal of integrating it into 40% of audits.

Implementation Planning and Program Management

The survey notes that 57%

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

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

SURVEY HIGHLIGHTS

In The IIA's 2018 North American Pulse of Internal Audit, 38% of respondents were not using data analytics, with 27% of these planning to do so. Two years later, the 2020 AAI survey shows the progress internal audit functions are making, including:

» 18% of audit teams have achieved a high level of maturity, using automated analytics across the organization, in cooperation with compliance and risk management functions.
» 26% rate their use of analytics as mature and well-managed.
» 26% are at an intermediate level.
» 18% occasionally use basic analytics.
» 12% do not use data analytics.

of teams have an effective approach to planning and managing the use of audit analytics. Successful teams implement a well-managed and communicated analytics program. A program addresses practical information for achieving the strategy and objectives such as acquiring skills, working with IT, getting data, and setting standards and processes.

Integrating Analytics Into the Audit Process Analytics can support virtually all aspects of internal audit's process. Surveyed functions use analytics most in control testing (65%), substantive procedures (59%), and audit planning (48%). Successful integration into the audit process requires planning and review at the beginning and end of an audit. Internal audit needs a systematic process for determining whether and how it will apply analytics in each audit stage.

Dealing With Data Obtaining timely and accurate data is a big challenge for 62% of internal audit functions. Nearly half of teams access a central audit data store. Having staff members who are skilled at identifying data requirements and extracting data without relying on the IT function is essential. Internal audit also needs efficient, independent, and secure processes for obtaining and storing data.

Analytics Usage and Technical Resources Hiring people with appropriate skills and knowledge, developing the analytics skills of existing staff members, and acquiring resources such as analytics libraries are crucial to the long-term success of analytics programs. More than 60% of audit functions have staff members who are capable of performing and developing analytics to meet most audit objectives. About one-third use a central library to encapsulate analytics knowledge, including suites of analytics and documentation to support specific audit objectives in specific areas.

Automation, Repeatability, and Sustainability Four out of 10 say they expect analytics usage to be sustainable and repeatable. At least 31% have had problems with sustainability, and 38% are aware of the risks of over-relying on specialists. Automation, documentation, and use of appropriate software are important in achieving sustainable and repeatable analytics.

Quality Assurance, Standards, and Reliability About half of internal audit functions have formal standards for ensuring the integrity of analytics and data, as well as for developing, testing, and documenting analytics. Without appropriate standards, analytics results may not be reliable for audit purposes. Organizations that lack those standards may be placing undue confidence in the accuracy of analytics results.

Organizational Structure and Skills Development Nearly half of internal audit functions surveyed rely on specialists to perform complex aspects of data analytics and to support nontechnical auditors in basic use. Another 31% rely on specialists for all analytics tasks. Additionally, 53% have analytics training programs and include development of analytics skills in auditors' performance objectives.

How audit functions organize specialists and integrate them into audit processes depends on the department's size and resources. Most audit functions implement a "blended" model combining specialists and nonspecialists, which continuously spreads knowledge and skills throughout the team.

Strategy and Leadership Are Key

Successfully using data analytics is vital to transforming audit processes. While some internal audit functions are making progress, many are still in the early stages of the process. These departments will need to address the eight issues mentioned above to achieve maximum benefits and sustain data analytics in their audits. Fully integrating analytics into core audit processes takes time to achieve.

Some important steps to establish a strong analytics program include a realistic strategy, goals, a practical implementation plan, and processes for integrating analytics into the audit. Although analytics involve many technical issues and skills, ultimately internal audit's success will depend on good leadership and management. Ia

JOHN VERVER, CPA, CISA, *is president of the Audit Analytics Institute in Vancouver, British Columbia.*

BY RICK WRIGHT

ASSESSING RISK IN A POST-PANDEMIC WORLD

Internal audit must recalibrate its risk alignment to respond to a dramatically changed risk environment.

As the coronavirus (COVID-19) pandemic has changed the world, internal audit functions have needed to face that world differently. Before the outbreak, internal auditors worked in similar ways, following the same code of conduct, adhering to the same standards, and using many of the same tools. Now, auditors have another thing in common: the need to adapt to frequently changing risk conditions.

COVID-19 has fundamentally changed the risk profiles of many organizations. As internal audit ramps up to a "new normal," it must recalibrate its audit plan from a dramatically different risk perspective.

An Audit Plan in Peril

Let's examine the timeline of events. Many internal audit functions started their risk assessment and audit planning process in late 2019. By early 2020, departments in most of the world had formed at least a skeleton of their audit plan, and some had communicated their formal plans to the audit committee and senior management. Some audit functions began executing engagements in early 2020.

That all changed in March, when the coronavirus began to race swiftly around the world and businesses experienced the first effects of social-distancing measures. Operationally, many organizations altered their business practices. From a compliance perspective, some regulatory requirements were suspended or relaxed for entire industries during the outbreak.

As these response measures quickly escalated, many audit functions drastically altered their audit plans. Businesses experienced so much disruption that it was nearly impossible to execute some audit engagements, or there simply was no value in doing so. Most respondents to an April 2020 IIA Quick Poll say they discontinued or reduced scope for some audit engagements, and nearly half canceled some engagements in response to COVID-19.

Four in 10 respondents indicate they redirected audit staff to nonaudit work. For some audit functions, temporary staff furloughs or budget reductions ended audit work or reduced staff activity to administrative duties.

Post-pandemic Planning

The audit plan that existed before the pandemic is based on an old risk paradigm. In a post-pandemic world, chief audit executives (CAEs) must think differently about their organizations' risks and how to redeploy audit resources. Here are some questions CAEs should ask in rethinking their audit plans.

What does the organization's new normal look like? Even businesses that were least impacted by COVID-19 will have systemic changes in their risk environment (see "Questions

SEND RISK WATCH ARTICLE IDEAS to Rick Wright at rick.wright@yrcw.com

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

QUESTIONS FOR CAES

To assess their situation during the COVID-19 crisis, CAEs should ask:

- » What does organizational staffing look like now? Have there been reductions or reorganizations?
- » Have key stakeholders changed? What new audit clients should I anticipate?
- » Have workforce reductions or reorganizations impacted how internal controls are executed? Are there new segregation of duties concerns or controls that no longer have control owners?
- » What processes have been temporarily or permanently changed?
- » What systems were temporarily modified or permanently changed? Were appropriate IT general controls followed for these changes, and, if not, what are the implications?
- » What controls were modified to accommodate unique business situations or risks?
- » Have there been any key personnel changes such as loss of unique subject-matter expertise or loss of key leaders in strategic areas?
- » Has the organization's strategic focus changed in the near or long term?
- » How have cost structures changed?
- » Have there been fundamental changes in the organization's debt and capital structures? Are there new or different debt covenants?
- » What new legal or compliance challenges is the organization facing (lawsuit exposures, changes to compliance infrastructure)?
- » Have new business opportunities emerged and have corresponding risks been identified?
- » Have the fundamentals of business-unit operations or strategies changed?
- » How have business continuity dynamics changed (key infrastructure changes, key customer changes)?
- » How have enterprise risk management dynamics changed (key risks, key risk indicators, response plans, and risk appetite)?
- » How have U.S. Sarbanes-Oxley Act of 2002 dynamics changed, including changes with external auditors, regulatory dynamics, and control owners?

for CAEs," this page). There may be major fallout to institutions and systems that organizations rely on, and regulators, financial institutions, and supply chains may experience disruptions well past the point when stay-at-home orders are relaxed. Some may no longer exist.

Is my risk assessment process agile enough? This question will be critical as CAEs begin prioritizing how to redeploy resources to address elevated risk in legacy risk areas as well as in new, uncharted territory. Risk assessments need to be agile because risk dynamics may change frequently in the near term. CAEs should evaluate and streamline legacy risk assessment processes.

Does my team still possess the skills to execute the risk assessment and audit plan? In the post-pandemic world, risk profiles probably will change—in some organizations, dramatically. CAEs need to evaluate the talent in their teams and internal audit's ability to identify risks and execute engagements that focus on new types of risk. They need to address questions such as:

- » How has internal audit's staffing changed?
- » Are staffing levels different, and have there been any changes in talent?
- » Are there new talent needs as a result of changes to the organization's risk profile?

Does my team still have an objective mindset? Unprecedented times call for unprecedented measures, and during the COVID-19 emergency, many internal auditors have been called to duty in ways they never imagined. If auditors were engaged in nonaudit activities within the business or performing activities that normally would be incompatible with professional standards, CAEs should evaluate staff objectivity.

A New World of Risk

The world is different now, with different risks. Internal audit functions must recalibrate how they view the inherent risks their organizations face as the recovery period begins.

Although pivoting from the old world to a new one is not a new phenomenon, the magnitude of COVID-19 impacts is more global and more severe than anything most auditors have experienced. Internal audit's ability to respond is vital not only to how its business recovers, but also how audit realigns with its stakeholders' needs. Ia

RICK WRIGHT, CIA, *is director, Internal Audit and ERM, at YRC Worldwide in Overland Park, Kan.*

Fraud Findings

BY WILLIAM BYRNE EDITED BY BRYANT RICHARDS

THE FRAUDULENT FINANCE OFFICER

When an executive abruptly quits her job, it sets off an internal audit that uncovers her five-year fraud.

Fabrina Carr joined CA Clubs, athletic and social clubs scattered throughout the Northeast, in 2012 as a secretary. Soon after, she was promoted to chief financial officer. As the financial director, she had overall control of the company's finances with little oversight, and she managed a small group of employees.

In late 2017, Carr phoned her work colleague from Bermuda to announce her resignation. This event, like any other unexpected executive departure, triggered an internal audit. The CEO of the company called Gina Cupler, the director of internal audit, whose team quickly started assessing the situation.

Internal audit requested emails and reports for corporate credit cards, travel expenses, and department expenses for the previous two years. Review of travel found significant and unusual spending activity, an excessive amount of expensive business trips, and a suspicious expense of $7,213. Cupler reviewed Carr's credit card statements and saw that the expense was paid to a funeral home. Public burial records revealed that Carr's sister had passed away and that the burial service was conducted by the funeral home noted in the credit card statement. A keyword search in Carr's email account captured correspondence with the funeral home, as well as an itemized invoice.

Cupler decided to dig deeper into CA Clubs' banking activity. Records indicated that Carr wrote checks to various people and vendors, yet the vendor master file did list those check recipients. When Cupler asked Carr's employees about the vendor master file, they told her that Carr maintained administrative control of the accounting system. This gave her unrestricted access to manipulate vendor records and transactions without detection. In addition, bank statements revealed five $100,000 wire transfers to an offshore account just before Carr resigned, which she approved herself.

Cupler notified the CEO of internal audit's findings and asked her team to expand the investigation to all five years of Carr's employment. Internal audit identified 1,464 personal transactions that started one month after Carr joined the company and carried forward for almost five years. Details of her unbelievable spending spree included 51 flights, 56 hotel stays, and 270 shopping transactions.

Cupler also inquired with the external auditors about their work over the past few years. Because the current external auditors had recently taken over the account, internal audit had to request copies of the audit reports from the

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

TO COMMENT on this article, **EMAIL** the author at william.byrne@theiia.org

LESSONS LEARNED

- A pre-employment background check is a key preventive control. Verification that a person is who he or she claims to be is important, especially when it comes to meeting the compliance requirements with hiring legally authorized citizens. The background check also provides an opportunity to check a person's criminal record, education, employment history, and other information to confirm its validity.
- Validation checks also should be performed when internal employees are promoted or move into new roles. Just because they have the skills, experience, and qualifications for the roles they were initially hired for does not mean they are immediately qualified for other roles in the company. HR should verify that their education, certifications, and any other skill sets are legitimate to meet the requirements of the new role.
- Reliance on a single person to control all aspects of financial transactions is never a good idea because it creates opportunities to commit fraud. Small organizations may need to get creative when it comes to segregation of duties. Board members for small not-for-profit organizations can take on an active financial governance role by reviewing financial information monthly.
- Thresholds should be in place around bank and credit card transactions with any override of these controls placed with the board. Companies also should work with their bank and credit card vendors to put automatic controls in place to prevent overspending.
- Small companies may not have the resources to look at the cultural aspects of their work environment. However, board leadership can have an active presence and provide employees with an outlet outside of their normal chain of command, such as a whistleblower hotline, to report suspicious or unethical activity.

previous auditors. The reports included findings about poor record keeping and insufficient evidence to support expenses and vendor payments. However, all interactions with the external auditors were through Carr, who never shared audit reports with the board. And the board never requested to see them.

Cupler was perplexed at how this could happen, so she instructed her team to perform more research into Carr's background. Her human resources (HR) file included a black and white copy of an accounting degree from Whatsworth College. An inquiry with the college found no record of Carr's attendance. The degree was forged, and HR never reviewed Carr's education or accounting certifications. The team then looked into Carr's criminal and past employment records, which revealed a history of theft and writing of fraudulent checks.

The incident showed what can go wrong without adequate checks and balances.

At the first evidence of fraud, Cupler notified the authorities and kept them abreast of developments. Carr was arrested at the airport upon her return from Bermuda and was questioned by authorities about the money that was missing. Carr claimed she loaned $500,000 to her boyfriend, a Nigerian man who she met online. A subordinate of Carr testified at the court hearing that Carr texted her outside of business hours instructing her to make payments to the man. Despite being suspicious about the payments, she felt bullied and did not want to question her supervisor. The prosecutor argued that these transactions were the reason Carr eventually resigned from CA Clubs—she had taken $500,000 to help her boyfriend leave Nigeria, but he never repaid her. The judge sentenced Carr to six years in jail, but she was not ordered to repay any costs because she declared bankruptcy.

CA Clubs sent an announcement to its 7,000 members sharing information about Carr's conviction and explaining that a new management structure was put in place with more rigorous financial processes to better protect the company. The incident was a painful reminder of what can go wrong without adequate checks and balances in place.

WILLIAM BYRNE, CIA, CPA, CISA, *is an audit and compliance professional in Spanish Fort, Ala.*

Navi

Arthur Piper

It may take years to calculate the full human cost of the coronavirus pandemic, but the pain is visible for all to see today. The U.S. has been hard hit. At the time of writing, there were more than 1.5 million confirmed U.S. cases of COVID-19 and more than 90,000 fatalities. Approximately 23 million people, representing nearly 15% of U.S. workers, had filed for unemployment benefits. Some parts of the country have ground to a standstill—a trend that has followed the progress of the virus around the globe.

Congress has thrown roughly $3 trillion at the problem with help for businesses and hard-hit citizens. Other countries have implemented similar fiscal initiatives. But despite

IMAGES: SKY, BLUEBEAT76 / ISTOCK.COM; ROAD, ROST-9D / ISTOCK.COM these essential measures, economists are divided on how fast economies will recover — not least because the virus has a habit of bouncing back once lockdown measures are relaxed. Parts of Japan reopened in mid-March, but are into their second period of restrictions. In Europe, Italy paved the way for four million people to return to work in early May: Manufacturers opened first, and now bars and hairdressers are emerging from two months of lockdown. Spain is in the early stages of its four-phase reopening, which regional authorities are implementing at different speeds. Many sectors remain closed across Europe, and the impact of lockdown grows by the day.

"This is much stronger in magnitude than the global financial crisis," International Monetary Fund chief economist Gita Gopinath has said. She told *The Wall Street Journal* in a video interview in April that economies will not pick up until the third or fourth quarters of 2020, but that will depend on whether countries can successfully emerge from lockdowns and stay that way.

The decisions organizations make now will help determine their survival in the short term. And for those that do survive, those steps will also lay the initial groundwork for recovery. Internal auditors can help organizations navigate the immediate risks, while keeping an eye farther on the

gating the Crisis

Auditors can help management address short-term risks, with an eye toward what may lie farther down the road.

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

horizon. They also can strengthen relationships with stakeholders and reinforce internal audit's value along the way.

SHARP CURVE AHEAD

The pandemic has already brought with it operating conditions that are potentially dangerous for both businesses and people. For example, as soon as Qatar put in place mitigation measures to protect citizens and residents against the coronavirus, businesses went into value-protection mode, according to Moses Chavi, chief audit executive (CAE) at a privately owned company in the region.

In particular, he says that two key themes have emerged for internal auditors and management—ones that are likely to persist during the forthcoming global recession this year: working capital management and talent management. The successful handling of these areas will play a crucial role in the eventual upturn.

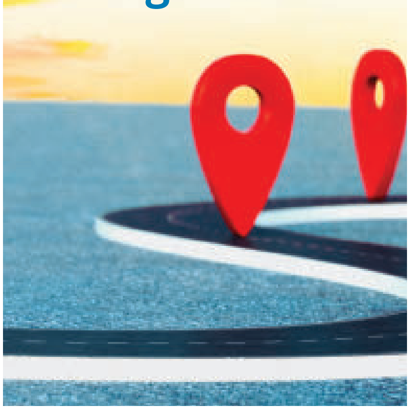
"Any company that has only a sub-optimal focus on working capital could see their businesses restricted to sustain fixed costs, including employees' salaries and the rent on operational sites," Chavi says. "And with much needed liquidity during the next three to six months, you will still have to catch up despite the fact the world will be entering an inevitable recession."

Similar to economic stimulus plans seen around the globe, locally Qatar's government has played a huge role to cushion economic activities and stimulate productivity through numerous incentives. Those include providing affordable financing and operational cost waivers, such as rentals, payroll support, and deferred loan repayments.

Chavi says he wonders whether businesses optimize costs without affecting their critical components, such as human resources. Finding creative ways of keeping people—such as constructive sabbaticals or by allowing more flexible working arrangements, whatever fits the ethos of the company—could be more expensive in the short term. At the same time, it could pay longer term dividends.

Since the crisis struck, Chavi and his internal audit team have been working flat out on adaptable working shifts fueled by coffee and adrenaline. His first moves were to start collaborating with the audit committee and

Two key themes have emerged for internal auditors and management: working capital management and talent management.



asking questions among corporate department heads and the financial and business leaders in critical areas of the company.

"We asked them what plans they had in all of the critical areas we had identified," he says. "Apart from doing a fresh risk assessment and pointing out things that they could not actually see, I'm trying to facilitate a stronger relationship between internal audit and the front-line entities."

RELATIONSHIP BUILDING

Chavi has become very active in committees—he was appointed to his company's crisis communication committee, partly to keep abreast of what was happening, but also to advise on how messages needed to be conveyed throughout the organization and beyond. "Internal audit has aggressively created relationships with other control teams across the entire business to make sure there is a common message going around about our monitoring initiatives," he says.

With social distancing policies in place, internal audit has changed its working routines. The team has used video to meet with managers and to carry out checks in such areas as sanitary controls, and employee and visitor screening, for instance. Chavi also has advocated for managers to make tough and timely decisions on, for example, which parts of their portfolios can be restructured, which need to be boosted, and where new lines need to be introduced to diversify and meet changing consumer behavior.

"Executives need to make sure they are aggressive in taking decisions," he says. "That also applies to business continuity plans, which may be irrelevant or outdated in the current situation and need radical overhauling." Chavi says he believes it is crucial to be "brutal with the truth" at audit committee meetings and at relevant executive management meetings.

But there have been some encouraging developments too. The organization's digital transformation has been enhanced by COVID-19, with some companies in the group moving rapidly into social media marketing, e-commerce, home deliveries, and adopting hand-held mobile and online payment. It is a move that he says has boosted customer experience. "Internal audit has had a keen interest in these processes, and we are making

More than 75% of U.S. adults would like to continue working remotely at least occasionally post-COVID-19, and 54% would like this to be their primary way of working, according to a recent IBM survey.

sure that we deal with the risks as they come along."

Chavi says that because his internal audit team has been able to hold management's hand through the crisis so far, and has refrained from judging in favor of providing practical solutions or constructive challenge, it will be well-positioned to continue helping in both an assurance and advisory capacity in crucial areas such as working capital management, talent retention, stakeholder relationships, cybersecurity, and data integrity.

"Internal audit needs to be visible and participate. You can't influence anybody without actually befriending them, without being close, without understanding and sharing their pain and troubles," Chavi says. "Applying your emotional intelligence is key to being able to influence the agenda and trajectory of risk management going forward so the business can survive and prosper in the future."

"Internal audit needs to be visible and participate. You can't influence anybody without actually befriending them, without being close. ..."

Moses Chavi

"Immediately after COVID-19, people are going to be thinking about the crisis and what they need to do to prepare for another pandemic. ..."

Alexander Larsen

FURTHER DOWN THE ROAD

The medium-term effects of the pandemic are going to introduce new uncertainties that could make recovery difficult, according to Alexander Larsen, president of Baldwin Global Risk Services, a risk consultancy with offices in the U.K. and North America. Businesses will need to assess and deal with altered social habits, customer expectations, new ways of working, and, in some sectors, unanticipated policy and regulatory changes, if they are to navigate these times successfully.

"Immediately after COVID-19, people are going to be thinking about the crisis and what they need to do to prepare for another pandemic—or whether they are prepared in the event that they lose their job due to the recession that will follow," he says. "They may be wondering why their homes are full of things that were absolutely useless in times of crisis, and that could affect their spending habits over the next couple of years."

Fear could also play a part in consumer behavior, Larsen says. Recent surveys suggest that when countries open up for business again, for instance, a large proportion of people will be scared of visiting crowded places. Three out of four people say they would now not attend trade shows or conferences in the future, according to a recent IBM survey. Some businesses may need to transform their operations into social-distancing friendly models where possible, Larsen adds.

In addition, many employees have learned that they can work from home effectively; some may prefer to continue doing so. Businesses that have been reluctant to be flexible may be forced into changing their policies to retain talent. Moreover, companies should not expect the business landscape to remain static as governments across the globe could take different views on tightening or slackening regulation from supply chains to financial contingencies. Political risk is also likely to increase.

"When I worked in Iraq during the construction of the world's largest undeveloped oil fields, the government often and unexpectedly instructed our company to stop buying products from certain countries, despite the strategic and financial significance of the project," Larsen says. "These were political decisions, often with valid reasons, and in the aftermath of COVID-19 it will be a more political world where such government sanctions could become more frequent."

Larsen says good risk management will be critical for survival and that internal audit has a key role to play in making that happen. Organizations will need a thorough understanding of their corporate and departmental risks, with a key focus on critical objectives, he says. They'll also need to examine where survival-level risks, or market-changing opportunities, are identified and linked to key risk indicators—essentially an early warning system for when things start to go wrong or relevant opportunities arise. Scenario planning, risk workshops, and horizon scanning exercises that focus on strategic risks and organizational strategies over the next three to five years must be in place.

RISK TOLERANCE

"Most organizations that are in a position of worrying about survival should forget about trying to set a risk appetite," Larsen adds. "They are having to take those risks anyway. The question is rather what levels of risk we can tolerate before the viability of the organization is threatened."

Key risk indicators should be introduced and linked to these risk tolerance levels—rather than appetite, Larsen says. That way, the business is put on alert when things start getting rocky.

But internal audit's support of risk management efforts is key. CAEs should use their influence at the board level to ensure the risk function is not tied down by processes and bureaucracy—risk management has to be dynamic. Internal audit also should provide assurance on whether management is implementing risk management's program. "Essentially, internal audit should be the risk function's ally by including risk management as part of their audits," Larsen says. "That will enable it to ensure that threats and opportunities are being identified across the organization and to ensure that they are being properly measured and controlled according to the risk procedures set by the risk management function."

MAXIMUM SPEED

Louis Cooper, chief executive of the Non-Executive Directors' Association, a board training and education, advisory, and support body based in London, agrees with Larsen that some businesses need to reappraise their approach to risk management. He has seen organizations begin to add a velocity factor to their risk matrices that traditionally only measure the impact and likelihood of risk: a dimension that he says needs to be incorporated into scenario planning, as it provides a speed of change component to the assessment of individual risks.

I'm not sure that governance frameworks have been tested in this way before, including in fundamental areas such as business continuity planning."

Louis Cooper

"Internal audit has an opportunity to provide real-time risk advice as businesses establish new processes in the 'new normal.'"

Esi Akinosho

In addition, others are moving away from the traditional enterprise risk management view and toward looking at risk in the extended enterprise. This approach takes further into account that many organizations increasingly rely on strategic partners, outsourced arrangements, and other third parties to take their products and services to market. Cooper agrees that internal audit should be undertaking more informed reviews of management activities and processes rather than doing test checks on individual business processes and transactions—following The IIA's long-held perspectives on risk-based auditing.

Cooper is concerned that an extended lockdown, or repeated ones, could mean that the accuracy of reporting and the information the board receives is compromised. Giving assurance in those areas could be equally affected. Without sending people out on location, internal auditors could be prevented from doing essential checks. In the U.K., the Financial Reporting Council's COVID-19 Bulletin March 2020 offers guidance to external auditors on such issues, which could be equally applicable to some internal audit assignments.

A TEST OF GOVERNANCE

Cooper also says that boards have been questioning whether their governance frameworks have been able to cope with fast-changing circumstances and whether they will enable their companies to be agile enough in the coming months and years. Some organizations, for example, have done a poor job of targeting their corporate communications and key business relationships—a clear indication that stakeholder groups and

Most businesses are not providing additional security training during the pandemic despite greater numbers of employees teleworking, according to a recent CrowdStrike survey.

contacts are inadequately mapped and understood. And some have fallen short in demonstrating whether executive leadership has had the right mandate to deal with unfolding problems. Other organizations have been unable to flex their business models—the way some fashion design enterprises were able to switch quickly from making clothes to making protective garments for health workers, for instance—and some have had difficulty with adapting to the culture shock of continuous remote working.

"I'm not sure that governance frameworks have been tested in this way before, including in fundamental areas such as business continuity planning," Cooper says. "People are very good at documenting things and putting them in the drawer without going through scenarios and checking that, if something were to happen, what the chain of command is and how it works in practice."

If internal audit has not been involved in those areas historically, boards will need them to take that role now, he says. They also will be looking for the function to assess how well the business has performed, identify gaps, and collate and disseminate the lessons learned to the board and management.

WORKING SMART

As well as participating on management committees dealing with business recovery, internal auditors need to work in a smarter, more focused way, says Esi Akinosho, EY Global Advisory Internal Audit leader. That includes following their businesses' lead in forcing rapid digital transformation.

"Internal audit has an opportunity to provide real-time risk advice as businesses establish new processes in the 'new normal,'" she says. "Teams can use predictive analytics to help identify emerging vulnerabilities and opportunities—this will give more timely value-add to management than traditional audit procedures."

She advises audit departments to focus on business-critical risks, especially cost recovery—such as working capital, cash management, vendor spending, and capital expenditure. Internal audit analytics can be applied to identify any cash recovery opportunities. That initiative also should extend to optimizing cost efficiency in the audit department itself.

"Internal audit should make its own contribution to the organization's cost diligence by optimizing the function's costs," she says. "Teams should take advantage of the technology momentum created by remote working to gain efficiencies across the internal audit life cycle. For example, digitize any procedures where possible and consider remote possibilities before spending on travel."

Where the internal audit function is less developed, or has issues with how its brand is perceived, it is time to act. "Organizations must start looking for opportunities to build the function's brand," she says. "For example, redeploy some resources to directly support business crisis management teams—this has the added benefit of building relationships and business knowledge simultaneously."

ALTERNATE ROUTES

Similarly, CAEs could build a more flexible resource structure in which, for instance, specialists are brought into the function for limited periods to provide additional expertise—either from within the business or from third-party providers.

"Internal audit has a great opportunity to help organizations transition out of the downturn by using the current disruption to accelerate transformation," Akinosho says. "Internal audit, as a profession, needs digitalization, a flexible people model, new skills, and a more dynamic approach that is more efficient and geared to giving timely insights on strategic risks."

Many businesses are going to have a life and death struggle with the effects of the coronavirus outbreak. Some will not make it. Those that do have their work cut out in streamlining portfolios and business processes; strengthening governance, risk management, and internal audit functions; and fast-tracking moves to make their enterprises digital—as well as keeping abreast of events and trends in the economy and among customers. Internal auditors have a key role to play in helping ensure their organizations make it along the road to recovery. If there was ever a time to demonstrate the true value of internal audit, it is today.

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

CAEs weigh in on the types of questions audit committees could ask them to strike the right tone.

Working in Concert

Neil Hodge

Illustrations by Edwin Fotheringham

The audit committee is meant to be one of the key champions of internal audit in any organization, so chief audit executives (CAEs) look to it for input, guidance, expertise, and feedback. But many CAEs say the audit committee should be more proactive in ensuring that it gets the best out of the audit function.

To do that, these CAEs say audit chairs should make more time for questioning the audit plan, as well as challenging internal audit about how effectively it can do the work it has been mandated to carry out. Many

audit heads also want audit committees to take more of a lead and bring more of their industry and boardroom experience into the meetings to make the audit process more robust.

Internal Auditor spoke to several current and former CAEs to find out which key questions they wish their audit committees would have asked them, but never—or rarely—did.

1. What can the audit committee do for you?

It sounds obvious, but CAEs say that in their experience, audit committee chairs rarely ask what they can do to support internal audit or make the function's job easier, such as requesting that senior management provide additional resources.

Liz Sandwith, chief professional practices adviser at the Chartered Institute of Internal Auditors in the U.K. and a former CAE, says, in her experience, audit committees are less challenging of internal audit's work than a CAE might expect.

"Audit committees don't always put themselves forward to champion internal audit within the organization, which is disappointing," Sandwith says. "They should be more proactive. Often, they just want the facts but don't ask any questions. A good audit chair will push to get more information and test the CAE by asking, 'Why aren't you looking at these areas?' and 'Why are you ignoring this?'" After all, if the CAE can't answer these types of questions, what level of assurance is the function really providing and how robust is the assurance the audit committee is receiving? she asks.

Sandwith also says that audit committees have been reluctant or slow to bring their outside experience and expertise to the table. "In the U.K., a lot of these people have either worked for or sat on the boards of FTSE100 companies, but they don't share that expertise," she explains. "None of them ever said to me, 'This is how our CAE used to manage internal audit' or 'In my previous company, internal audit did X, Y, and Z.'" Audit committee members usually have chief financial officer (CFO), CEO, external audit, and blue-chip corporate experience, but they don't use it to the committee's advantage, something Sandwith considers a wasted opportunity.

"The relationship between internal audit and the audit committee is a unique one," says Harold Silverman, managing director of CAE services at The IIA and a former vice president of internal audit at fast-food chain Wendy's. And that relationship often is one-sided: The CAE reports what is happening, and the audit committee listens and takes those views on board and perhaps asks management about some of the issues. Silverman says that he was rarely asked by the chair of the audit committee what he or she could do to help with internal audit's work, or how to improve its standing in the organization or with management. "Those attitudes are changing now," he adds.

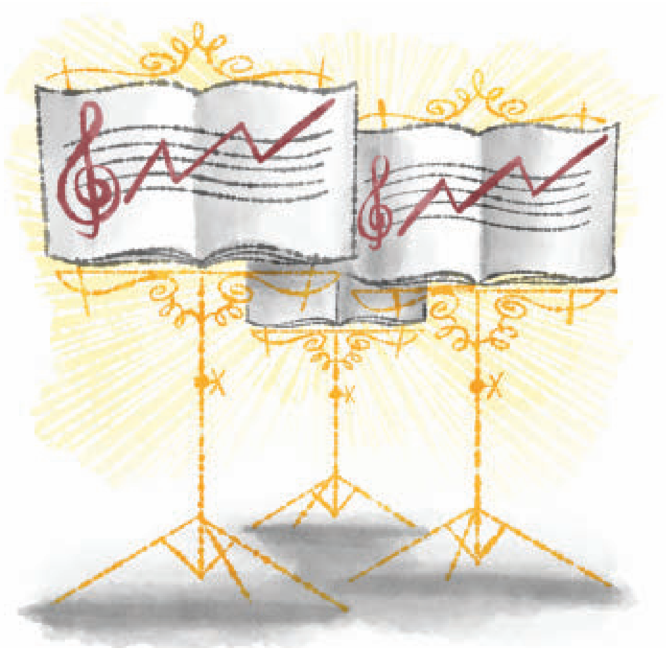
2. Is the audit plan the right one, and can it be delivered?

CAEs say audit committees rarely question whether the approved audit plan is actually the right one for the business—even if the risk landscape or circumstances impacting the business have changed.

"Audit committee chairs do not see themselves as managers," Silverman says. "Instead, they see their role as reviewing and overseeing a process that has already been agreed on with management, and which, therefore, must presumably be the right one to satisfy the needs of the business."

He adds that audit committees rarely question management's thinking about the audit plan or ask internal audit whether the plan should change in light of new events or information. "Indeed, some chairs actually want internal audit to work out any problems with the plan before they take it to the audit committee because they don't want to second-guess management," he says.

Sandwith agrees. "It has always appeared to me that the audit committee has just presumed that, as the CAE, the budget and the audit plan as presented is the final version, it meets with the resources that we have, and doesn't need to be discussed," she says. "They simply don't question the process behind the audit plan." Sandwith says the audit committee should check whether the audit plan is going down the right path for the business and that internal audit can do the work effectively with its budget and resources.



3. Does internal audit have the necessary resources and skills to provide the required level of assurance?

CAEs say there also is a presumption that just because an audit plan spells out what an internal audit function is meant to do over the course of a year, such work will be carried out to the letter and to a high standard. Not so, experts say.

"Management may want internal audit to look at a range of areas

Less than 20% of respondents say their audit committee is highly interested in internal audit's innovation and transformation activities, notes Protiviti's Embracing the Next Generation of Internal Auditing.

to provide assurance, but it does not necessarily follow that the function is only capable of doing so within the budget and skills it currently has," Sandwith says. "A lot of the areas under review will be complex, such as cybersecurity, and while internal audit can check whether there are suitable processes and controls in place, many functions will not have the level of technical expertise to provide the kind of assurance that some organizations—particularly those in highly-regulated industries—will need." Additionally, if the audit plan is too optimistic and contains too much work for the function to realistically do well, it will lead to internal audit simply performing basic box-ticking compliance, which is of no use to anyone, she adds.

Bethmara Kessler, a former CAE and currently chair of the Association of Certified Fraud Examiners' Board of Regents, says a good way for audit chairs to test an audit plan's effectiveness—as well as the capabilities of the CAE and the audit function—is to ask two budgeting questions: 1) If the committee gave internal audit an additional 10% of its budget, how would the funds be used and why? And 2) If the committee cut 10% of the budget, where would the CAE make cuts and why?

"That kind of questioning focuses the CAE to explain where the key risk areas are, and what amount of resources need to be dedicated to them to ensure that the appropriate level of assurance is achieved," Kessler says. "It also can help open up a discussion about what issues keep the CAE awake at night, and how those concerns can be addressed."

Kessler says audit committees also should ask internal audit functions whether they have the technical skills to review emerging risks, particularly in fast-moving areas such as technology. "Blockchain, machine learning, and artificial intelligence present both risks and opportunities," she explains. "As a result, internal audit needs to keep pace with developments in these fields and look at what the organization is doing to leverage the benefits and identify and mitigate the risks. Audit committees, therefore, have a right—if not a duty—to question their competence."

4. How responsive is management in dealing with the risks that internal audit and other assurance functions flag to them?

Internal audit, risk management, compliance, and in-house legal may be great at highlighting problem areas and emerging risks that need to be controlled, but if management—which is ultimately responsible for managing risk—does not follow through with the recommendations from assurance functions, then the whole exercise can be pointless. However, CAEs say that audit committees do not always ask how responsive management is about putting these recommendations into action, or how effectively they do it.

"Internal audit can make as many recommendations as it likes to implement controls, but if management does nothing, it is a wasted exercise," says Sarah Blackburn, a former CAE at several FTSE100 companies and now a nonexecutive director at U.K.-based RAC Pension Fund Trustee. "Similarly, it is equally a waste of time if internal audit overwhelms management with dozens and dozens of actions to be taken."

Blackburn says audit committees need to ensure that internal audit is clearly prioritizing key actions for management to implement, and that management duly does its part. This means audit committees need to raise questions about management's

"Audit committees don't always put themselves forward to champion internal audit within the organization, which is disappointing."

Liz Sandwith

"There is no harm—but potentially enormous benefits—in asking the CAE whether the external audit firm is delivering a quality audit."

Bethmara Kessler

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

responsiveness, and CAEs need to be prepared to give an objective account of management's actions.

Kessler adds that "internal audit is the third line of defense and it is in a unique position to provide a clear and objective assessment of how well management accepts its role as being ultimately responsible for risk management within the organization." As such, she says, the audit committee should be asking internal audit to report regularly on the status of actions that management has and has not implemented as a result of audit's work.

5. What is internal audit's view of external audit and other assurance functions?

Internal audit is just one of the functions reporting to the audit committee. Others include risk management, compliance, in-house legal, and external audit. Yet, CAEs say that they are rarely asked whether they work alongside these functions, and if so, how frequently they might share information and ideas, or if there is any overlap in work. Nor is internal audit asked to give an opinion on these functions' effectiveness, though audit committees often ask external auditors to provide an opinion on the organization's in-house functions.

> **There is an opportunity for the audit committee to find out what the CAE's vision is for the department.**

"I don't think in my time as a CAE I have ever been asked by an audit committee chair whether we regularly meet or work alongside the other assurance functions or discuss risks with them," Sandwith says. For example, she might tell the audit committee that internal audit met quarterly with the head of risk management and spoke often with other assurance functions, but the conversation ends there. "I've never been asked to explain what our relationship is like with them, or whether it can be improved, enhanced, or encouraged further," she explains.

Kessler agrees that audit committees need to ask for internal audit's perspective on external audit, in particular. "Audit committees should consider internal audit an expert on audit in general and should ask for its opinion on external audit's work," she says. "There is no harm—but potentially enormous benefits—in asking the CAE whether the external audit firm is delivering a quality audit."

Blackburn also says that audit committees need to ask more questions around the quality of risk reporting by assurance functions. "Audit committees need to make sure that internal audit provides them with a professional opinion about how risks are reported and controlled across the organization," she says. For example, audit committees need to ask whether these functions see risk in the same way. Do they report, identify, and manage risk in the same way? Does the organization understand and evaluate risk in the same way across all its operations? Audit committees need to be satisfied that there is consistency in risk understanding and risk reporting, she adds.

6. How can internal audit add value? What is your vision for the function?

Internal audit's workload entails more than agreeing on an audit plan and completing it. The profession has made enormous strides in demonstrating it can be a value-adding function, and CAEs say that audit committees should encourage this further.

Bryant Richards, an associate professor of Accounting and Finance at

An **open** relationship between the audit committee and internal audit **best positions** the function to help the organization reach its goals, says The IIA's Relationships of Trust position paper.

Nichols College in Dudley, Mass., and former director of corporate governance at the Mohegan Tribe, which owns casinos and other organizations, says that it would have sent a powerful message if the audit committee had asked him, "How can you go out there and add more value?"

Rather than focusing largely on compliance and areas such as Sarbanes-Oxley controls, Richards says, "If the audit committee had pushed internal audit to get more involved in supporting business strategy, that would have sent a very powerful message to management that the board trusted us and that our skills were being underused." It also would have moved internal audit from defense to offense and would have increased its credibility and value within the organization. That kind of backing may have prompted other functions to engage with them more, too, he adds.

Richards explains that audit committees also should ask CAEs to explain what their vision is for the audit function for five or 10 years. There is a real opportunity for the audit committee to work with the CAE and find out what his or her vision is for the department—how internal audit can expand its role; provide wider, deeper, and better assurance; help support the overall strategy implementation; and get involved in new areas. It would help transform internal audit into a much more proactive and strategic force within the organization, he says.

7. Would you like to have a coffee off-site?

Asking questions unofficially can be a more effective way of finding out information than asking CAEs to provide answers in a forum with tight time constraints. Some CAEs say that audit committee chairs should approach them separately to establish an informal relationship where they can talk openly and raise concerns and ideas in a more relaxed setting.

"Audit chairs need to encourage CAEs to speak freely about any concerns they may have about the audit plan, risk management, and any other business," Blackburn says. "Even though internal audit is supposed to be independent and objective, it can still be difficult for CAEs to talk through their concerns in an audit committee meeting with limited time and where key executives—especially the CFO—also may be in attendance."

An off-site meeting may encourage the CAE to speak more openly, and it may provide a useful opportunity for both parties to get a better understanding of each other's priorities and key concerns, she adds. Alternatively, a virtual one-on-one discussion may suffice.

DON'T ASK, DO TELL

The experts agree that audit committees are getting better at asking more questions around the topic of internal audit—but they add that more can still be done.

Yet, CAEs also can take better charge of the situation. If they think that the audit committee has missed an opportunity to ask deeper or more pertinent questions, there is an obvious course of action—give them a prompt. To do this, CAEs should act as if they've been asked the question they think should have been asked, supply the answers or follow-up, and make clear what recommendations they feel the audit function should act upon to address the key issues. At best, the inclusion of such details will force the audit committee to discuss the issues being raised. At worst, the committee will think the points raised are part of "business as usual" and will agree with the proposals. Ia

NEIL HODGE *is a freelance journalist based in Nottingham, U.K.*

"Audit chairs need to encourage CAEs to speak freely about any concerns they may have about the audit plan, risk management, and any other business."

Sarah Blackburn

"If the audit committee had pushed internal audit to get more involved in supporting business strategy, that would have sent a very powerful message to management."

Bryant Richards

Data Protection in a GDPR World

New privacy regulations require increased data vigilance, expanding the need for internal audit's risk and control expertise.

Victor Chavalit
Lindsay Hohler

OMELCHENKO / SHUTTERSTOCK.COM

Over the past decade, data has become the most important asset for companies. Big-data analytic capabilities and advancements in artificial intelligence have shifted business models and transformed how companies use information. And with data growing exponentially every day, the task of protecting it has become more and more challenging.

The passage of new regulations such as the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) in the U.S. imposed new requirements for how companies use and collect personal information. Noncompliance or failure to adequately safeguard personal information can result in significant fines and impact the corporate brand and consumer trust. As a result, internal audit is increasingly being asked to help evaluate data protection risks and controls.

Although many companies have implemented protection capabilities to comply with the requirements, laws are still being interpreted—and what constitutes adequate security under CCPA and GDPR is still being analyzed. Organizations must maintain their focus and monitoring efforts to remain compliant. Internal audit teams can help companies identify risks, improve controls, and work as a strategic partner in evolving data protection capabilities.

DEFINE DATA PROTECTION

Data protection refers to the practice of safeguarding information from compromise, loss, and disruption. In the context of GDPR and other privacy regulations, the concept focuses on protection of personal data. And it isn't limited to just preventing that data from being hacked or stolen. The scope of data protection ranges from classification and categorization to retention of all data in an organization.

Companies need to understand the sensitivity and type of data they collect, process, and store. Moreover, they need to ensure data is available and appropriately retained based on business need. Given the broad scope of what data protection can entail, internal auditors should ensure their organization has established a governance model with defined roles and responsibilities for each team as well as procedures that detail the steps necessary to protect data. At the same time, these procedures should align with compliance and security objectives.

To help achieve this alignment, internal auditors should define a baseline framework that allows roles, activities, and controls to be mapped to specific requirements or domains. Auditors can leverage industry frameworks, such as the U.S. National Institute of Standards and Technology (NIST) Privacy Framework or International Organization for Standardization's ISO 27701 framework, to support the development of privacy controls. Defining a framework and tailoring it to the company will help ensure that only the necessary requirements are considered and tested. The framework also will enable internal auditors to identify the accountable party for each requirement or domain.

DETERMINE AUDIT SCOPE

In defining the scope for a data protection audit, it's important to take a risk-based approach. Internal auditors should conduct a risk assessment to determine the inherent risk for each business process and system and prioritize audits of higher risk areas. The results can help determine the audit frequency for each business process and its systems.

From a data protection standpoint, the risk assessment should consider exposure factors and threats to these processes and IT systems. Internal auditors can assess several factors:

- The type of information being processed.
- The sensitivity of the data.
- Whether the process or system is external facing.
- The volume of data being processed.
- The number of users who have access to the data.
- Whether an internal or external party hosts or manages the supporting IT systems.

From a threat perspective, internal auditors can refer to industry frameworks such as Microsoft's STRIDE—primarily focused on security threats—and the LINDDUN privacy threat modeling framework developed by the DistriNet and COSIC research group at Katholieke Universiteit Leuven in Belgium. Alternatively, auditors can build their own threat and vulnerability register. They can then map the threats to each business process and system to support the inherent risk calculation. Prioritizing the business processes and systems will help internal auditors maximize their effort and investment while providing company leadership with clear visibility into critical business operations and data protection risk areas.

> **Auditors can map the threats to each business process and system to support the inherent risk calculation.**

UNDERSTAND THE DATA LIFE CYCLE

To identify data protection gaps and test control effectiveness end-to-end, internal auditors should tailor their approach to the data life cycle. Auditors should develop a standard approach based on each life-cycle stage—such as data collection, transfer, use, storage, and destruction/retention—and then customize the approach for each business process and its systems. This effort will help streamline the planning and design phase, allowing auditors to focus on the execution and control testing phase of the audit.

One-third of all nations lack laws to **protect** their citizens' online **data** and privacy, according to the United Nations Conference on Trade and Development.

Understanding the life cycle provides internal auditors with insight on why data is being collected, where it's being transferred, how it's used, where it's stored, and when it's destroyed. Without this context, controls are implemented and tested in silos, making the efforts ineffective or redundant. Auditors should use this information to evaluate the risk of each business process and its systems in relation to the corresponding data protection controls.

Through the life-cycle approach, internal auditors also can evaluate the data subject right-request process. Under GDPR and other new privacy regulations, individuals—referred to as *data subjects* in GDPR—have the right to request access to their information or have it deleted. Many companies struggle to fulfill these requests due to a lack of understanding about where personal data is stored or if it can be deleted. Through a data life-cycle lens, internal auditors can provide assurance on whether IT systems are appropriately scoped to support data access or deletion requests.

Although there are tools available that can help companies discover and scan IT systems to consolidate and analyze data, gaps in knowledge of each system may still exist. Understanding the full data life cycle can help uncover data that may be stored in the cloud or with other third-party providers. Internal auditors should identify these gaps and work with the privacy and compliance teams to develop a plan for incorporating those data repositories into the company's data subject right-request processes.

DATA PROTECTION BY DESIGN

As a best practice, data protection needs to be incorporated into the design process at the onset—a concept known as *data protection by design*. While data protection traditionally was most often delegated to information security and involved managing point technology solutions—products that solve or address one specific need—such as data loss prevention tools, this narrow scope limited companies' ability to put in place effective controls. The concept of data protection has evolved as a result of GDPR and other privacy regulations, expanding the scope of protection measures.

Data protection by design focuses on identifying issues and risks throughout the entire data life cycle and implementing controls as the business processes are being developed, rather than at the end. By evaluating the entire life cycle, internal auditors can identify gaps in data protection controls and help pinpoint the life-cycle stage where these controls should be implemented.

Data protection by design does not mean that companies need to develop new processes and questionnaires that ultimately inundate the business with additional work. Instead, data protection requirements and controls should be woven into the process itself. They should be integrated into existing processes when a company evaluates a vendor, when a new solution is being designed, or when a business process changes. Internal auditors can use their broad knowledge of the organization to help companies design a process that promotes a culture of compliance while limiting business disruption.

Training and oversight efforts represent a good starting point to begin incorporating data protection by design concepts into the organization. Internal auditors can work with human resources (HR) and privacy teams to develop meaningful training programs and awareness campaigns. The training content should be relevant to each group of employees and focus on how they can apply data protection into their daily activities. Audit results

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

can be leveraged to pinpoint areas that pose a higher risk to tailor the training content. By providing training content that is applicable to employee roles and daily responsibilities, companies can shift the way employees think. Privacy, data protection, and other compliance requirements become a part of their job instead of an extra component.

Consider, for example, an IT developer whose role is to build a customer web application. Through training that is targeted to her role and responsibilities, the developer can be made aware of privacy and data protection requirements for collecting and storing personal data. When the developer subsequently creates a mechanism for data collection, she will know that a method to collect consent should be in place, along with notice to inform data subjects of how the data will be processed and the need to adequately protect data being stored. Understanding these requirements at the beginning can provide privacy and compliance teams with ample time to evaluate and provide accurate requirements and content to business and IT teams, such as: Should the system be designed to provide opt-in or just opt-out consent? What encryption controls need to be in place? How long should data be retained?

In terms of oversight, having the right privacy and other subject matter resources—e.g., security, legal, and HR—accounted for early on in the process can help identify requirements and controls that may be missing from the design. The internal audit team can work with the various departments to form a review body tasked with evaluating new initiatives and IT systems. Inserting this body into the software development life cycle and tying funding or resources to the approval process can help ensure all new initiatives and IT systems are being reviewed. Additionally, having internal audit participate in these review sessions can be beneficial when performing control testing.

The internal audit team can help form a review body tasked with evaluating new initiatives and IT systems.

DATA PROTECTION DURING THE PANDEMIC

As part of efforts to combat COVID-19 and protect human lives, many governments and companies have implemented emergency procedures. This has created some confusion and concern around privacy and data protection requirements, given the use of personal data such as health information and geolocation. In response, the European Data Protection Board released its Statement on the Processing of Personal Data in the Context of the COVID-19 Outbreak to provide guidance to governments and companies regarding the processing of personal data. The statement can be helpful to internal auditors as they navigate their organization's compliance with GDPR.

In a period where decisions and response time are critical, internal auditors can also provide the necessary support and guidance to company leadership so that privacy and data protection requirements do not act as a hindrance to implementing emergency

Approximately **half** of U.S. adults have decided not to use a **product** or **service** because they were worried about collection of personal information, according to a Pew Research Center survey.

procedures. For example, auditors can develop control decision trees—charts or data flow diagrams that consist of logic decisions and possible outcomes (controls or activities)—to help inform business and IT teams of requirements and considerations when collecting, processing, or storing personal data. Decision trees can provide a systematic way of identifying options that are least intrusive to individuals.

GDPR and other privacy regulations should not impede the organization's ability to carry out and implement emergency functions. Instead, companies and internal auditors should use the privacy requirements as guidelines for ensuring adequate controls are considered and implemented to protect the privacy rights of individuals during these unprecedented times.

PREPARING FOR THE FUTURE

Privacy and data protection regulations will continue to mature globally. GDPR has created a strong foundation in Europe, while the U.S. landscape is still developing with other states and the federal government following California's lead. Other regions in the world have started to introduce or pass their own privacy regulations, such as the Brazilian General Data Protection Law and India's Personal Data Protection Bill. Internal auditors can help companies rationalize the different requirements to streamline assessments and control testing, which will improve efficiencies for many businesses.

Furthermore, as more data and IT systems move into the cloud and company technology boundaries continue to expand, it is harder to define responsibility and accountability for data protection. Taking a purely reactive approach toward new regulations and requirements puts companies at risk for noncompliance. The internal audit function can work with company leadership to help the entire organization embrace the concept of data protection by design, which can ensure appropriate controls are evaluated up front, protecting the organization, its employees, its customers, and their data. Ia

VICTOR CHAVALIT, CISSP, *is cyber risk senior manager within the Advisory Services practice of Grant Thornton LLP in Chicago.*

LINDSAY HOHLER, CIPP/US, *is cyber risk principal within the Advisory Services practice of Grant Thornton in Arlington, Va.*

The IIA's 2020–2021 North American Board chair, NANCY HAIG, says CAEs can take steps to ensure their internal audit functions live up to the high standards to which they're held.

Building a GREAT team

Photographs by Doug Scaletta

It seems as though internal audit is one of those functions where the actions of just one person on the team tend to shape the perception of the full team—especially if those actions are negative. When it comes to internal audit, it is imperative that all team members are able to competently represent the function, as well as the profession. Seen as a group, and held to a high standard of integrity and objectivity, internal auditors must earn the trust and respect of their stakeholders. So, how can we build a great team, where each individual is skilled, professional, and personable, regardless of whether there are only a few members or more than 500?

Great internal audit teams embrace diversity, have the right skills, support team members, and understand that each team member is a leader in the organization. Great team leaders promote training and attainment of the Certified Internal Auditor (CIA), implement a Quality Assurance and Improvement Program (QAIP), and ensure work conforms with the *International Standards for the Professional Practice of Internal Auditing.*

Working this year as chair of The IIA's North American Board, I will be reminding practitioners of the responsibility to become their professional best to enhance their internal audit teams. This is important, as our members represent and serve not only their organizations, but also the profession.

DIVERSITY IS KEY

An important key to building a great team is having diverse team members—diverse in maturity, experience, thought, culture, background, interests, and skills. I have always been able to assemble the most diverse teams. How? Because I always choose the candidates who have the competencies needed to perform in the role, the capacity and interest to want to learn, and a demonstrated ability to work as a team member. Looking for differences among these candidates, rather than similarities, helps build a great team. It is important to provide these criteria and rationale to all who are involved in the hiring process, so all can learn what is truly valued.

WHAT SKILLS ARE IMPORTANT?

One of the most important skills for internal audit professionals, at all levels, is communication. All team members should be skilled in oral and written communication, including interviewing, report writing, and presentation. Team members also should demonstrate the ability to think critically and objectively to identify issues and potential actions to resolve those issues.

Additionally, team members must keep abreast of changes in their organization, industry, and profession. Today's important risk areas include cyber, privacy, anti-bribery, and corruption—but these risks will constantly evolve, and others will emerge. That is why the focus should be on individuals' desire and ability to be continuous learners.

Also, it's important to have team members with skills and interests in different areas. For example, I have always gravitated toward regulatory compliance, and enjoyed monitoring changes in laws and regulations that affected my organization. This may be because I began my career in the financial services sector, which is highly regulated. However, I have worked with other team members who equally enjoyed learning everything they could about IT, accounting proclamations, business processes, contracting, etc. The trick is to harness these diverse interests to build the team, while ensuring all have the right competencies.

THE RIGHT CREDENTIALS

Obviously, because we are in the internal audit profession, the CIA is the premier certification to demonstrate an understanding of what we represent and how we go about our work. Other certifications and licenses also may be important to demonstrate that the individual has the initiative and drive to continue learning, and to demonstrate his or her skill in a particular area of interest. These include the Certified Fraud Examiner, Certified Information Systems Auditor, Certified Compliance and Ethics Professional, Certified Public Accountant, etc.

Again, those differing and specific interests will add to the effectiveness of the team as a whole. If a team member is not ready to pursue the CIA credential, participating in the annual internal quality assessment can be a great way for the individual to at least learn the *Standards*.

SPEAKING OF QUALITY

I am a firm believer that a QAIP, when implemented appropriately, can be a positive factor for both the team and the individual. The QAIP can help ensure that work is being performed in accordance with the *Standards*. It also can provide support if there are questions about the internal auditors' independence and objectivity.

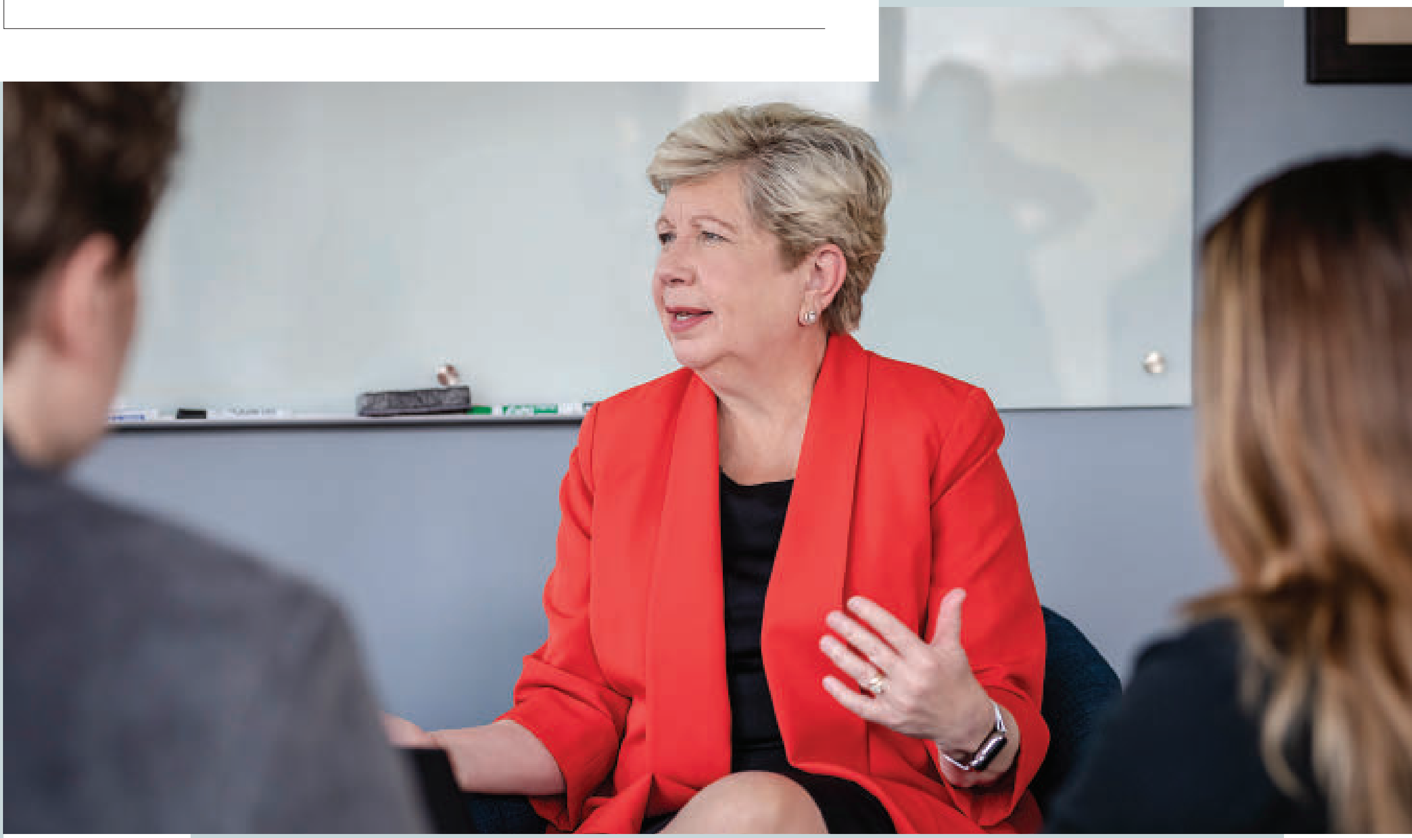
Internal client surveys highlight how and where the function is adding value, as well as areas of improvement, for either the team as a whole or for an individual. Additionally, having a QAIP in place sends the message to clients that the internal audit function cares about how its work is performed. Also, if an external assessment is performed, we have a good answer when we get the question, "Who audits the auditors?"

OPPORTUNITIES FOR LEARNING

Once team members have been hired, it is imperative that each individual receives training to help develop specific areas of strength and interest. The IIA provides numerous opportunities through conferences, seminars, customized on-site programs, chapter programs, and webinars.

Additionally, individuals should be expected to learn as much as possible from others in the organization. In fact, CAEs may assign individual team members as liaisons to specific departments or functions, particularly where they have an interest. Team members should be encouraged to continuously

Team meetings are another valuable source of learning and training for internal audit functions.



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

read and perform external research and share this information with business leaders, resulting in valued professional relationships with key stakeholders.

Team meetings are another valuable source of learning and training for internal audit functions. All team members should be encouraged to speak up and openly share their successes and challenges. Others should share how they have overcome similar challenges. Hot topics or emerging risks can be assigned to individuals who can research them and present their findings during team meetings, thus practicing their presentation skills.

CAEs also can rotate the leadership of team meetings among those who are in the process of developing their management skills. Those individuals should plan the meetings, including developing the agenda and facilitating the discussion among team members. The CAE should train the potential leader to be inclusive and supportive of other team members, so that the right environment will continue in the future.

Training should occur during the execution of each project. CAEs should allow team members, to the extent possible, to pick the projects that they would like to perform. Some team members are anxious to learn about a new area, while others may be content to audit something they may have previously reviewed—because they know they don't currently have the expanded bandwidth. Allowing for and understanding when team members want to grow, or when they need to temporarily scale back, creates an environment where all feel supported. Consequently, that feeling evolves into loyalty, engagement, and productivity.

WHEN IT GOES WRONG

Mistakes happen. But, before they do, CAEs should teach their teams how to address mistakes. If team members feel supported, and able to communicate, they will speak up when a report or comment needs to be retracted.

CAEs should be certain team members know that they've taken the right action by acknowledging and communicating the error. They should include them in making the correction, while acknowledging that as the leader, the CAE is ultimately responsible for any mistakes made by the team. The CAE should share the retraction or other resolution to ensure he or she is sending the message that this is the expected action when an error occurs.

LEARNING FROM CONFLICT

Unfortunately, more than once, a team member has come to me upset about treatment received from a "higher-up." My response is to objectively look at the situation as one would an audit observation. First, the auditor should go over the facts.

FROM TEAM PLAYER TO TEAM LEADER

When I began my career, I did not know what an internal auditor was. I was offered a position as an internal auditor at JPMorgan Chase & Co. (formerly Chemical Bank) in New York City after graduating from Wagner College in Staten Island, N.Y., with a Bachelor of Science degree in economics/business administration. At that time I had no idea what the work would entail. All I knew was that it was one of two positions offered to recent college graduates that would expose them to many different areas of the bank (the other being credit training), and that it was supposed to be a stepping stone into a position in bank operations.

For me, though, it was the start of my internal audit career. Even then, our CAE, the late Richard Hulbert, was focused on risk. He encouraged us to read the Federal Register each day to understand the rules that would impact the organization and what corresponding changes (policies, procedures, etc.) would need to be implemented. He also encouraged us to read *The Wall Street Journal* daily, and if something had gone wrong at another institution, he expected us to examine our bank's internal operations to understand what controls (and yes, that was the word we used, even then) would need to be implemented to prevent a similar situation.

I loved the work, the continuous learning, and the focus on all kinds of risks inside and outside of the organization. I was promoted several times, and enjoyed hiring and helping others succeed. I was encouraged to pursue my first certification, the Chartered Bank Auditor, and my first MBA (management and finance), all while I was at the bank—and that's how it began.

I later earned my CIA when I decided I wanted to pursue my earlier interest in health care, and spent some time in internal audit in that industry. I found that leadership and internal audit skills were also transferable to the pharmaceutical and professional services industries.

My internal audit career has taken me around the globe, and I have had the opportunity to visit approximately 30% of the world—with hopefully more travel to come! In my last role, as head of internal audit and compliance for a global consulting firm, I was able to implement an internship program with a local college that continues today. I am a current participant in The IIA's Emerging Leaders Mentoring Program, and I am hopeful that I will have further opportunities to mentor others and introduce them to a career that can be both fun and fulfilling.

Internal auditors, more than anyone in the organization, are expected to act professionally and with courage, humility, and integrity at all times.

Could he or she possibly have done something incorrectly, or unprofessionally? If the answer is no, further examination of the situation is required. Could the individual exhibiting the bad behavior be under stress that may have caused an inappropriate reaction, especially if the person is acting out of character? In those cases, I advise the team member to allow the situation to cool down and to re-approach the person with my support, if he or she feels capable. I encourage the team member to attempt to resolve the conflict, anticipating that he or she may need to acknowledge what previously occurred, accept responsibility, if warranted, and be proactive in seeking resolution.

If, on the other hand, there is no excuse for the behavior, and the person has a reputation for behaving or responding inappropriately, I will call out the behavior. Together, the team member and I will identify exactly what was inappropriate about the behavior, and we will discuss the best course of action for addressing the situation. In most cases, the root cause of inappropriate behavior is bullying, which I then offer to address for the team member, to ensure he or she feels supported.

EVERYONE IS A LEADER

One of the most important messages for internal audit team members is to know that, regardless of title or position, each team member is a leader. Whether team members are aware or not, their behavior is being observed and assessed by others, and the expectations are high. Internal auditors, more than anyone in the organization, are expected to act professionally and with courage, humility, and integrity at all times. They are expected to be good communicators, analytical problem-solvers, and highly competent, as well as exhibit a passion for the profession.

MORE THAN EVER

Especially in these challenging times, internal auditors must come together as a strong team. Internal audit functions need to assist their organizations as new strategies, objectives, processes, and procedures are developed—putting forth a team of trusted, competent, and valued professionals. Ia

NANCY HAIG, CIA, CCSA, CRMA, CFSA, *was most recently the director of internal audit and compliance for a global consulting firm in New York.*

Transforming Corporate Card Audits

Several robust technologies can provide greater efficiency and insights on card transaction audits.

Bonnie Tse

One of the most significant changes in auditing corporate card expenses over the past decade has been the conversion of supporting documentation from paper receipts to electronic form. Although an internal auditor's core duties of ensuring completeness and accuracy in record-keeping remain the same, the electronic form has altered the dynamics of those duties significantly.

Not so long ago, people mailed paper receipts to a central location for processing. Today, by contrast, a simple receipt photo, screenshot, or email confirmation uploaded via a website or mobile app often suffices. The convenience and efficiency of electronic files, as well as enabling technologies such as cloud storage, data visualization, and automation, have created both new opportunities and challenges in auditing corporate card transactions.

TO COMMENT on this article, **EMAIL** the author at bonnie.tse@theiia.org

Cloud Storage

Cloud storage is an on-demand, self-service model where data or software as a service is stored remotely on virtual servers hosted by third parties.

Opportunities Cloud storage removes the storage limitation challenge presented by retaining physical copies of paper receipts or using on-site servers, as it is easily scalable to accommodate any data storage needs. Additionally, it reduces pre-installation costs and maintenance charges associated with on-site servers.

Duplicate back-up copies of data can be stored in multiple locations worldwide, making data less vulnerable to natural disasters. Cloud storage also makes it easier to implement a document retention period for physical receipts. Corporate card data that requires long-term storage could be archived or automatically purged after a defined period.

Limitations Digital documentation is susceptible to malicious software, such as ransomware, that encrypts data to an unusable form and holds it hostage unless payment is made. Focusing on data security may protect transaction information from hacking, which could result in negative publicity from a data breach or give competitors insight into prospective projects.

Use, transfer, and purge of stored personally identifiable information attached to employees' expenses is limited by regulations such as the European Union's General Data Protection Regulation and the California Consumer Privacy Act. If the data is backed-up or stored in international locations, there is the added complexity of the local regulations around the data's use.

Depending on how the information is housed and structured in a third-party's platform, organizations may have to pay extra to fully access their data the way they want. For instance, application programming interface (API) software, which allows two applications to talk to each other, often is an extra cost. API, for example, allows the expense repository system and audit software to talk to each other and is used to access features or data of a service application.

Data Visualization

Data visualization distills large datasets into visual graphics to allow for easy understanding of complex relationships within the data.

Opportunities Combined with data analytics, data visualization allows the data to be dissected in more ways than before. For example, a dashboard template could track multiple key performance indicators linked to a database that would allow users to slice the data in real time and filter down to focus on any variable for specified business areas.

Beyond simply graph or pivot data in Excel, data visualization can simultaneously overlay multiple variables, such as transaction types, on a geographic map while highlighting the magnitude of the transactions in different sizes and colors. This could be used, for example, to target potential fraud indicators where there may be misalignment between travel plans and expense transaction locations.

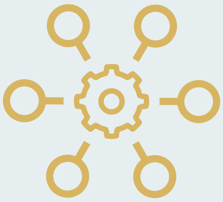
Auditors can use data visualization to add value in addition to investigating noncompliance. It could highlight frequent exception trends and indicate broader implications, such as the need for additional employee training for specific parts of the corporate card policy or the need to amend the policy. For example, the corporate card policy may have a standard flat threshold for specific expense types, such as lodging or business meals. However, the policy does not consider that guideline amounts are not realistic for high-cost-of-living areas, such as New York or San Francisco, and may indicate that the policy needs to be amended to allow for fluctuations. Data visualization could help draw attention to these types of trends.

The data also could highlight opportunities to reduce costs and negotiate group rates if, for example, it finds that cross-departmental employees frequently attend the same conferences or events. On the other hand, it could flag individuals who did not use the prenegotiated group rate, and management could use it as an opportunity to educate those employees on ways to maximize their budget.

Limitations Despite these benefits, there is a risk of overreliance on data visualization. The insights gleaned from it are limited by the accuracy and completeness of the data inputs, false positives, or misleading trends if used incorrectly.

83% of occupational frauds fall under asset misappropriation—inflated expense reports, false billing schemes, and theft of cash—according to the 2020 ACFE Report to the Nations.

Automation



Processes that can drive efficiency and cost savings in corporate card audits include robotic process automation (RPA), a software robot that mimics human actions; machine learning (ML), a subset of artificial intelligence (AI) that allows systems to learn new things from data; and AI, the simulation of human intelligence by machines.

Opportunities The combination of RPA, ML, and AI creates a system that mimics human judgment in defined circumstances and could reduce time spent on repetitive and low-value tasks. With the advent of these technologies, the audit concept of reasonable assurance due to limited available audit hours and resources could move much closer to absolute assurance. In the past, internal auditors have focused on rigid criteria: a specific time period, an individual's or group's transactions, keywords, or transactions that exceed a defined threshold. Many potential noncompliant transactions that fall out of the hard-line criteria would be missed, and without software with AI capabilities, it would be impossible for auditors to review the entire volume of transactions.

Expense tracking software could incorporate a company corporate card policy so that RPA could continuously monitor and flag noncompliant transactions for additional approval or auditor review. This would ensure that auditors focus on transactions that are more likely to be exceptions and perform more meaningful work.

Optical character recognition (OCR) image-reading software could save not only the submitter's time, but also the approver's and auditor's time, by automatically pulling and matching the amounts from the uploaded receipt to the reported expense transaction. For international receipts in foreign languages, the software can translate the language, look up the local tax rates, and calculate currency exchange rates. More advanced expense-tracking software could cross-reference publicly available data, such as online menus or historical hotel rates, to determine the reasonable range for specific expenses. This would allow for variation due to seasonal or location-based fluctuations for the reasonable expense threshold range.

AI with OCR could detect split transactions where a larger receipt is paid through multiple transactions or using multiple corporate cards. Another instance of split transaction could occur if there were a deposit that was paid in advance and the remainder of the balance was paid at a later date. Image-reading software could easily detect this, while it is much harder for an auditor to find with paper receipts. The use of OCR software could reduce excessive payment for the same expenses submitted multiple times or circumvention of the policy expense guideline amount.

Another AI capability is systematic risk profiling. Low-risk recurring transactions could be auto-approved and bypass the need for manager review, saving hours of administrative time and increasing the time available for more productive tasks. This time could focus on high-risk individuals or departments more likely to be noncompliant, leading to increased policy education or behavior change.

Limitations AI, ML, and RPA are relatively new and often expensive technologies. The software is only as good as the training data set inputs and what it is being programmed to do. AI involves a learning process, where users must "train" the software. Moreover, the AI tools may produce a high number of false positives, which could create more work than traditional methods. If these technologies do not detect pervasive noncompliance in the training data set, the model may never catch it—but a person could.

ML and AI are susceptible to biases and skewed results because of bad data inputs. For instance, the technology might determine that a certain gender or race is a higher risk for noncompliance, leading auditors to focus on those individuals' transactions and possibly result in legal issues/consequences.

BEYOND COMPLIANCE

Auditing purchase card expenses goes far beyond reviewing for policy compliance. By using the cloud, data visualization, and automation in corporate card audits, auditors can drive better stewardship of company resources. While these technologies provide tremendous benefits, it's important for internal auditors to be aware of their downsides to adjust accordingly. By building on this foundation, internal audit also can use these technologies to transform the audits of other business areas and processes.

BONNIE TSE, CIA, CISA, CPA, PMP, *is a senior internal auditor at T-Mobile in Bellevue, Wash.*

More than ever, internal audit needs to reconsider, measure, and communicate its true value to the audit committee and management.

Adding Value 2.0

Nicodemus Tan

In the current environment of cost-cutting and changing priorities, internal audit will be challenged to demonstrate its value to the organization. Yet, the value of internal audit is hard to fathom. If the audit function's core value lies in helping the organization reduce risks, how does it quantify and report on losses averted when risk events did not occur?

As internal audit's value proposition expands beyond its traditional assurance boundaries, audit functions have an opportunity to rethink how they contribute to the business. While many facets may be intangible, internal audit can use recognized metrics to demonstrate its tangible value to audit committees and senior management.

CURRENT NOTIONS OF VALUE

In communicating to the audit committee, many internal auditors have measured and shared work completed as a proxy for value delivered. They have used the quantity of audit projects performed, cycles covered, or number of issues raised and reported as key performance indicators (KPIs).

However, work completed does not necessarily correlate with value delivered and may distract stakeholders from the actual value delivered. It also is easy for internal audit to inflate such a single facet of quantitative data by sacrificing quality. For example,

ILLUSTRATIONS: Z_WEI / ISTOCK.COM

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

audit functions could limit the scope of reviews to increase the number of audits or the number of cycles reviewed.

Many internal audit functions use the balanced scorecard method to measure performance and communicate their value. It is a useful tool to translate internal audit strategy into actionable plans, with detailed metrics to show progress. However, most of the metrics commonly used in balanced scorecard or other forms of assessment relate to the execution of internal audit plans and may not measure value accurately.

Take for example the perceived quality of internal auditors based on their academic qualifications or years of experience. Although experienced auditors with strong academic achievements may be considered more likely to deliver value, this metric may not reflect the actual value those auditors delivered. Similarly, another common KPI is the completion of audits within budget, a metric that is important for cost control but does not measure value.

WHAT IS VALUABLE TO STAKEHOLDERS?

It is difficult to score a goal when one does not know where the goal post is. To provide and communicate value, internal audit must first identify what its key stakeholders—the audit committee and management—deem valuable.

While internal audit reports functionally to the audit committee, the discussions and agreement with senior management about its value proposition are no less important. Senior management is closer to the business and provides powerful independent feedback on internal audit to the audit committee.

Given the profession's advancement over the past decade, the value of internal audit is no longer limited to the recommendations auditors provide. Likewise, discussions of value should go beyond assurance over internal controls. Internal auditors can assess what stakeholders find valuable in several ways.

Review Stakeholder Topics As the chief audit executive (CAE) prepares to discuss value drivers with the audit committee and senior management, a good starting place is to review recent communications. Requests by the audit committee and senior management or seemingly run-of-the-mill interactions that were not captured by current metrics may indicate value drivers.

Seek Feedback Formal discussions with the audit committee and senior management about the value proposition should take place at least annually. Common methods for gathering feedback include electronic surveys of individual stakeholders, face-to-face or phone interviews, and facilitated focus group discussions with the audit committee and senior management. These discussions can be conducted separately or jointly.

Where practical and meaningful, a focus group discussion involving the CAE may be preferred. Unlike a survey, this interactive format can uncover an individual's blind spots, encourage cross-pollination of views, and build consensus among stakeholders.

If conducted well, surveys or discussions with middle or lower management following each audit can provide timely responses. These clients often are the original and unfiltered source of feedback for senior management. Responses about what internal audit did and did not do well can enable the department to fine-tune its value proposition and better match the value management seeks, which can change throughout the year. The responses also are a great source of information for the CAE's annual discussions with the audit committee and senior management.

Discuss Value During the discussions about internal audit's value, CAEs and their auditors should note that there is a fine line between proposing suggestions or alternative views and appearing to promote their self-interest. Even in situations where management's requests seem unreasonable or irrelevant, internal audit should ask questions to clarify the intent of the proposal rather than reject the notion outright and be seen as defensive.

> **Where there is material misalignment, feedback can be a golden opportunity to identify an expectation gap.**

Where there is material misalignment, the feedback can be a golden opportunity for internal audit to identify an expectation gap. While it is uncomfortable to hear negative feedback, it is important to interpret it correctly and constructively to retain the client's trust and enable a more collaborative partnership. Otherwise, clients may decide that internal audit will not act upon their feedback.

ACKNOWLEDGMENT-BASED METRICS

Once internal audit has agreed with its stakeholders on the value proposition, it should develop metrics on a reciprocity basis. This means the metric should

52% of CAEs say their function is at the managed and optimizing levels of the Internal Audit Maturity Model, but 20% are at the two lowest levels, the 2020 North American Pulse of Internal Audit reports.

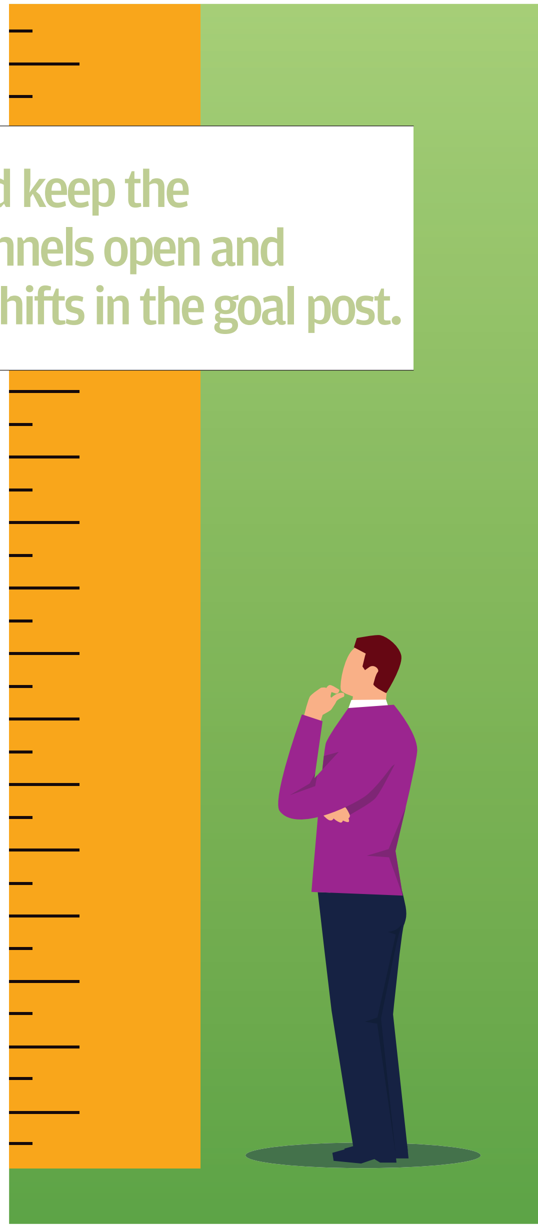
not be a measurement that is determined solely by internal audit but also includes acknowledgment and affirmation by management.

Talent An increasingly recognized value internal audit provides is a talent pipeline. Many organizations have either actively recruited internal auditors to join their business functions or included internal audit as a rotational stint in their management trainee programs. If management does not perceive this as valuable, it would not offer these positions to auditors. Correspondingly, the number of auditors who are offered business function positions is a good indicator of value generated and acknowledged by the organization.

Training Well-established internal audit functions often train process owners on risks and controls, but management may not always consider this valuable. One way to assess and report on this value is to collate information on the number of attendees and their feedback. Using a consistent grading scale to compare across time and regions, such feedback could indicate the value the training provided.

Process Improvement Many organizations practice the Six Sigma approach of reducing defect rates in a product, process, or service. To measure internal audit's value, management could adopt this methodology by comparing the error rates of processes before and after business units have undertaken remedies recommended in an internal audit report. For example, Six Sigma practitioners can compare the error rate or near-miss rate of dispensing medication at a pharmacy before and after it has implemented a maker-checker control that internal audit suggested. Conversely, management may only measure error rates for processes that it considers to be key risk factors, as error rates of other processes would not demonstrate value.

Consulting High-performing internal audit functions often are involved in value-enhancement projects such as IT system design discussions and pre-acquisition due diligence. Internal audit's participation in these consulting projects are typically at management's request, which indicates that management realizes internal audit's value.



Internal audit should keep the communication channels open and check in about any shifts in the goal post.

Analytics Expertise Another source of value is internal audit's use of analytics. Auditors often share the insights gleaned from these techniques with management following the completion of an audit. As this becomes a standard practice, many internal audit functions have progressed to coaching and transferring these techniques to management, which is a convincing sign of value.

COMMUNICATING VALUE

The unique environment of each organization and the dynamic role of its internal audit function mean that there are far more ever-changing sources of value. To stay relevant, internal audit should keep the communication channels open and check in periodically with the audit committee and management about any shifts in the goal post.

To maintain credibility, internal audit must not cherry-pick its metrics. It should not just report regularly on metrics that are under its direct control and

78% of "digitally fit" audit functions develop new services for the organization and stakeholders, and 80% change the audit plan more frequently than in the past, according to PwC's 2019 State of Internal Audit.

report selectively on all other positive information only on an ad-hoc basis.

A good practice is to set relevant metrics for each of the agreed-upon value drivers based on acknowledgment-based results and confirm them with the audit committee. For example, rather than the number of training sessions conducted for management, internal audit could monitor training feedback from attendees. Instead of using the number of audits performed with data analytics, the department could use the number of data analytics scripts adopted by management.

Internal audit should provide these metrics to the audit committee and management periodically, regardless of the actual score. Moreover, it should provide them before beginning the annual management survey of internal audit to facilitate a more accurate assessment. Then, internal audit should report the results of the annual management survey and the metrics together to the audit committee to give a full picture of the value the department has delivered.

Where internal audit has fallen short of certain KPIs or its metrics are not up to par, it should not appear defensive or attempt to boost numbers in the short run. Instead, auditors should understand the underlying value proposition. For example, if the number of internal auditors hired by business units decreases, the CAE should pause in promoting the team to the business owners. During this time, the CAE should ask management if the type of skills that the business is seeking has evolved or if the audit staff's training is sufficient for auditors to add value to the business.

CONVINCING STAKEHOLDERS

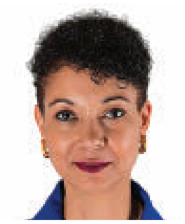
In the current business climate, the risk landscape of organizations is changing at an unprecedented rate, as are the expectations of internal audit's key stakeholders. To deliver a greater level of value, internal audit needs to reconsider its value proposition from a blank slate, starting with stakeholders' current expectations both now and in what may be a radically different future. A candid, open, and consistent approach to identifying, agreeing upon, and reporting on internal audit's value proposition can make the most persuasive case for the function's value. Ia

NICODEMUS TAN, CIA, CRMA, CFSA, CA, *is a partner at Baker Tilly LLP in Singapore.*

BY MATT KELLY

COVID-19: THE ULTIMATE GOVERNANCE CHALLENGE

The global scope and growing duration of the coronavirus pandemic make it a formidable menace for corporate boards, management, and internal audit to address.



SHELLYE ARCHAMBEAU

ALPA PARIKH

WENDY PFEIFFER

In many ways, the coronavirus (COVID-19) pandemic is the corporate governance crisis we've been preparing for all our lives. It is a public health crisis that has caused an economic crisis, which for many organizations has also caused operational or liquidity crises.

Its consequences dwarf the financial crisis of 2008 and the Sept. 11 attacks combined. It is global in scope and unending in duration. And yet, corporate boards, management, and internal audit teams have to confront this menace somehow.

We can start with the obvious: Board directors are as bewildered as everyone else by COVID-19. Clearly the pandemic challenges organizations in all sorts of ways, and directors do grasp that point—but understanding the exact ways COVID-19 will challenge their businesses is no small thing.

"For many, this particular risk—basically, of businesses completely shutting down and everyone staying home—well, that wasn't on the risk profile," says Shellye Archambeau, who serves on four corporate boards, including Verizon and Nordstrom.

That puts corporate directors in a delicate position. From management, they want to hear about new information, new risks, or new plans being executed, and that can be a lot; Archambeau figures she has been on board-related calls at least once a day, if not more. At the same time, however, directors don't want to burden management too much, since the executive team has plenty to do already.

"It's very important at this unusual time to trust management, and let them do their job of running the company," says Alpa Parikh, who was chief audit executive at Puget Sound Energy until last fall and now serves on the audit committee of a Seattle-area social services nonprofit. Her operating principle these days: Don't ask unnecessary questions of management; do think about the long-term implications of short-term actions the organization takes to keep operations alive right now.

That makes sense. Ill-advised actions today could constrain a company's strategic choices tomorrow, next month, or next year—and that's what a board is supposed to prevent. Its job is to preserve the organization's ability to create value for stakeholders. In that case, several issues rise to the top of corporate directors' concerns.

Keeping Things Going

Foremost are questions about the organization's cash position, and its ability to continue as a going concern even if COVID-19 drags on for many months. (And let's not kid ourselves, it probably will.) So for

READ MORE ON STAKEHOLDER RELATIONS visit InternalAuditor.org

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

example, one specific priority would be an organization's ability to preserve the cash it has. That means directors will want to know about spending and hiring freezes, and also about approval processes for significant expenditures — including whether those processes are sufficiently tight, given the company's projected cash flows.

Then again, Wendy Pfeiffer, on the audit committees of cybersecurity firm Qualys and consulting business SADA, says companies can't forget about "market moments" either, such as the chance to pick up a merger target on the cheap or to launch a new line of business. You can't do those things without cash, so cash preservation is important; but directors also want to know that management is trying to maintain strategic perspective and flexibility, too, so the company can jump on a good moment when one arises.

OK, that concept is easy enough to grasp. Here in the real world, however, audit committees are trying to understand such issues while the economic ground keeps shifting. Well-understood key performance indicators or key risk indicators might no longer fit. Models of expected customer behavior, sales cycles, liquidity, or supply chain risks could all unravel.

> **The ability to plan, even under today's enormously difficult circumstances, is what keeps an organization alive.**

Directors are acutely aware of that possibility, and want assurance that management — and audit teams — are trying to stay ahead of such shifts. That means lots of scenario-planning. "Leverage your analytical skills to figure out what the scenarios might look like and capitalize on strategic agility," Parikh says.

And audit committees still have their day jobs overseeing the financial reporting function. Regulators have published a laundry list of accounting items that could be difficult to calculate these days, and those items are sure to be concerns for the audit committee, too.

Among the issues flagged: lease modifications if a company starts giving back space (which could actually goose the organization's income statement upward), impairment of goodwill or intangible assets (which could wallop the income statement and the balance sheet), revenue recognition, hedging, and more. COVID-19's effect on those items will involve a lot of subjective judgment. Audit committees will want to know that said judgment is sound and grounded in good data, as much as possible.

Internal Audit's Role in Continuity Today

As companies are scrambling to understand what their new risks are, and how to amend business processes to keep those risks at acceptable levels, internal audit has an important role to play. It is internal audit's job, after all, to perform critical assessments of emerging risks, use data analytics to build monitoring tools, and counsel management on possible changes to business processes. "That focus on data and specificity is massively important," Pfeiffer says.

Internal audit can especially look at technology risks, including ones that might arise from adopting new work-from-home processes in haste. Those are crucial corporate capabilities as COVID-19 continues.

"We already have those skill sets that allow us to adapt quickly to things like this," Parikh says. "That overview is very important right now, when you can look at processes end to end, across different functions and areas within a company to assess risks and identify potential opportunities."

That's the nub of the COVID-19 challenge for organizations, really. Success isn't about having a business continuity plan per se, because those plans never match the disaster you actually face. They only bring the shortcomings in your plan into sharp relief. The *ability* to plan, even under today's enormously difficult circumstances, is what keeps an organization alive.

It's also what audit committees want to see from management teams: an ability to observe changing conditions and devise a response that won't trap the organization in a strategic or operational dead end.

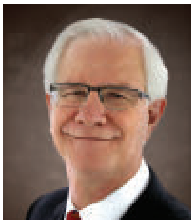
"I'd rather have the human brain," Pfeiffer says. "I'd rather have people who are aware and engaged and have their own early-warning system and expertise and creativity." Then let those people collaborate their way to a feasible solution, "rather than work their way through a playbook."

Those are words for an audit team to live by. And if the first weeks of COVID-19 are any indicator, we'll be living by them for quite some time. Ia

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

To keep up with the latest news for internal auditors regarding the coronavirus, visit the COVID-19 Newswire on InternalAuditor.org. For additional helpful resources related to the pandemic, visit The IIA COVID-19 Resource Exchange on www.theiia.org.

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



BY J. MICHAEL JACKA

BRAND AWARENESS

Among clients, is your audit function top of mind as an enabler of success?

Here's a quick marketing lesson. An organization's success is closely tied to its brand, and determining the public's awareness of a brand is best achieved through four measures: aided recognition, unaided recognition, aided consideration, and unaided consideration. Aided recognition measures how many people recognize a brand when it is presented to them. Unaided recognition measures how many include the brand when asked for the names of organizations that provide similar goods or services. Aided consideration measures how many say they would use the brand when it is presented as an option. Unaided consideration measures how many name the brand, unprompted, when asked where they would turn for a particular good or service.

That last measure is marketing's holy grail. When a brand achieves unaided consideration, it means people know the brand and consider it when making their choices. For example, when people shop for insurance, on average they call three companies. Insurance companies, therefore, want to be among the top three brands in unaided consideration.

Suppose a person walks into the C-suite and asks one of these four questions:

- "Have you heard of the profession of internal audit?" (recognition)
- "Which departments help organizations achieve their objectives?" (unaided recognition)
- "When you want to ensure your objectives are being met, would you turn to internal audit?" (aided consideration)
- "Who would you turn to for help in ensuring your organization's success?" (unaided consideration)

How would your internal audit department fare? Are you in the top three? Does the C-suite even know you exist and that you can provide help?

These are the difficult questions internal auditors must be willing to ask themselves. Even when we brag that our clients come to us for help, what does that really mean? Do they only come when there is potential fraud, when there is a control breakdown, or when adding internal audit to the project team seems like the friendly thing to do? That's a nice start. But we need to consider whether internal audit is top of mind for our clients and if including us in all efforts toward achieving success is second nature for them. Do they realize that the ultimate service we provide is helping the organization succeed?

We have to market ourselves, constantly pushing the value we provide. Sometimes these efforts are explicit—"Look what we've done!" Other times the approach is more subtle—providing quality that cannot be ignored. But we must ensure that everyone sees that value and becomes increasingly aware of internal audit's capabilities. We have to reach the point where we not only crack the top three, but we are far and above everyone else at the No. 1 spot. 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

Eye on Business

HOME WORK

Agility is key in both remote work and the new normal following the pandemic.

ERNEST ANUNCIACION
Director of Product Marketing
Workiva

ANDREW STRUTHERS-KENNEDY
Managing Director
Leader, IT Audit Practice
Protiviti

How should audit plans change when the entire organization is working from home?

ANUNCIACION There are two components to this: what's in the plan and how to execute the plan. First, the chief audit executive (CAE) will need to adjust the scope of the audit plan, which could mean an emergency meeting with the audit committee and executive management, or maybe a special session with the audit committee chair to reprioritize. What may have been important at the beginning of the year may not be critical today. The CAE should determine whether to remove, postpone, or even cancel engagements, and decide what can be accomplished given the timeframe and new realities of working from home. Second, how is internal audit going to complete the audits? If auditors can't visit a location, or if they can't do a walk-through in person, consider what technologies the organization has to assist with conducting the fieldwork. There are plenty of online meeting and collaborative tools that can help. If anything, this highlights the need for internal audit teams to be agile, and technology is a big part of that.

STRUTHERS-KENNEDY CAEs have been actively promoting their ability to be agile and responsive to a dynamic work environment. Recent events provide an opportunity for audit leaders to "walk the talk" with their teams. Leaders need to apply tools and techniques to facilitate strong communication and increase the monitoring of company activities in a new and remote environment. On the topic of tools, many audit functions had been making concerted efforts to advance analytics and technology-enabled auditing. The need to make increased use of tools and data has never been greater. Internal audit functions should look for every opportunity to apply analytics and other techniques to enterprise data sets to help them accomplish their own risk assurance objectives, as well as provide any necessary support to the broader business.

What key risks should internal audit functions be focused on during times of crisis?

STRUTHERS-KENNEDY Beyond the risk of degradation of the broad system of internal control driven by remote working and reduced workforces, two broad risk areas are notable on top of the recurring business risks to any company. The first area includes those looking to exploit the crisis through a fraud or data breach. Bad actors will look for any weakness in controls or oversight that may have been compromised in a time of crisis. In addition, well-meaning employees may now be working in ways that compromise privacy and data protection policies. The second area is in the rapid deployment of new processes

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

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

and technologies, including changes made to existing technologies through emergency processes, to facilitate a remote workforce. A thorough—but appropriately rapid—assessment should be conducted to understand the potential exposures and related controls. On a broader and more sustained basis, audit functions must develop a more dynamic and responsive approach to risk assessment.

ANUNCIACION If internal audit has a risk-based audit plan, the approach doesn't necessarily change as the key risks addressed should still align with the organization's strategic objectives. The crisis may force internal audit teams to look at risk much more broadly, such as at an enterprise level—a level or two beyond process-level risk. CAEs also may need to add audits that address areas where there was not risk coverage on the original plan, especially for teams that spend the majority of time on U.S. Sarbanes-Oxley Act or internal control over financial reporting testing. Areas such as business continuity, supply chain, IT, cybersecurity, and operations come to mind.

How should internal auditors be thinking about independence and objectivity in a time of crisis?

ANUNCIACION Auditors are very well equipped to identify and assess risk and can help the company plan for any situation, but there's a line past design and operating effectiveness. Internal audit can't implement or make final decisions based on any recommendations; that is management's responsibility. Accordingly, CAEs might shift the plan from less compulsory or assurance type of audits to more advisory and consultative engagements. That type of perspective shows there are ways in which internal audit can maintain independence and objectivity while adding value to the organization.

STRUTHERS-KENNEDY In these extraordinary times, audit functions should work to provide the best support and partnership possible, delivering on the core mission to protect the enterprise from undue risk while also focusing on bringing extra capacity and capability, which may in some instances result in direct support for core and critical business operations. Internal audit's skills and talent can be helpful in assisting the organization to manage through the crisis, whether those talents are applied to risk assurance activities or, in certain cases, hands-on operational support. Where audit is being asked to provide operational support, this should be done with approval of executive management and the audit committee, including a discussion and plan for how any objectivity or independence conflicts that may be created will be addressed.

What types of training should internal auditors take advantage of when working from home?

STRUTHERS-KENNEDY The use of next generation tools, including those used for collaboration, automation, analysis of large and complex data sets, and methods such as agile and design thinking, are needed today. Auditors should take every opportunity to increase their knowledge and skills related to capabilities and features of platforms such as Microsoft Office 365—which includes a wide ranges of features that are beneficial to remote work—collaboration tools, and data analytics and automation platforms and methods. There is no shortage of training material available online, much of which is high quality and free.

ANUNCIACION This is a great time for auditors to knock out items on their laundry list—things that they may not have had time for in the past. Internal audit can do a self-assessment on its current methodology. Perhaps the CAE has been meaning to implement a quality assurance and improvement program—it's the ideal time to do that. Internal auditors should consider taking an online course on data analytics or other technical areas, so that when we do come out from this, they've gained knowledge to broaden their horizons.

What can CAEs do during a pandemic to be better prepared when employees return to the office?

ANUNCIACION In the short term, it's all about focusing on team and employee morale. We don't always know what's going on in our staff's personal lives. CAEs should be sensitive to those unknowns. They may be experiencing a lack of childcare. Perhaps they have a friend or a relative who was diagnosed with the illness. They may be feeling some financial pressures. CAEs should be flexible in terms of demands and what they're looking for from their teams. Longer term, it's all about perspective. What concessions or modifications to the culture of the team will need to be made once they come back to the office? Is working from home going to be expected? How do CAEs incorporate what they've learned in preparation for future emergencies?

STRUTHERS-KENNEDY It can be hard to focus on anything but the challenges and stresses of a crisis, but within this situation—and perhaps even because of it—there is plenty of innovation occurring and opportunity being revealed. Rapid deployment of collaboration technologies, cross-functional and cross-border teams coming together and working through complex situations and decisions in rapid fashion, making better use of data and tools where people and other resources are not available, and working in highly agile and responsive ways are all good examples. Through these pursuits, CAEs are building resiliency into their own departments. The workplace we return to may well be very different; therefore, it's critical the office of tomorrow is shaped to reflect elements of our remote world today. Ia

IIA Calendar

Please check the website for more details on all of The IIA's in-person events, as they are subject to change.

IIA CONFERENCES

www.theiia.org/conferences

AUG. 17–19
Governance, Risk, & Control Conference
JW Marriott Austin
Austin, TX

SEPT. 13–16
IIA-Canada National Conference
TELUS Convention Centre
Calgary, Alberta

SEPT. 14–15
Financial Services Exchange
Omni Shoreham
Washington, DC

SEPT. 16–17
Women in Internal Audit Leadership
Omni Shoreham
Washington, DC

NOV. 2-4
International Conference
Fontainebleau
Miami Beach, FL

IIA TRAINING

www.theiia.org/training

JULY 6–15
Fundamentals of IT Auditing
Online

JULY 7–16
Audit Report Writing
Online

JULY 7–23
Tools for New Auditors
(New)
Online

JULY 13–22
Cybersecurity Auditing in an Unsecure World
Online

JULY 14–23
Root Cause Analysis for Internal Auditors
Online

JULY 28–31
Statistical Sampling for Internal Auditors
Online

AUG. 3–12
Enterprise Risk Management: A Driver for Organizational Change
Online

AUG. 4–13
Operational Auditing: Influencing Positive Change
Online

AUG. 4–20
Tools for Lead Auditors
(New)
Online

AUG. 10–12
IT General Controls
(Updated)
Online

AUG. 17–28
CIA Exam Preparation - Part 2: Practice of Internal Auditing
Online

AUG. 18–27
Advanced Risk-based Auditing (Updated)
Online

AUG. 24–SEPT. 2
Fundamentals of Risk-based Auditing
Online

SEPT. 8–17
Fundamentals of IT Auditing
Online

SEPT. 8–24
Tools for Audit Managers
(New)
Online

SEPT. 9
Fundamentals of Internal Auditing
Online

SEPT. 9–18
Root Cause Analysis for Internal Auditors
Online

SEPT. 10–11
Data Analysis for Internal Auditors
Online

SEPT. 14–23
Cybersecurity Auditing in an Unsecure World
Online

SEPT. 14–25
CIA Exam Preparation – Part 1: Essentials of Internal Auditing
Online

SEPT. 15–24
Critical Thinking in the Audit Process
Online

JULY/AUGUST/SEPTEM

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

PHOTO: RAWPIXEL.COM / SHUTTERSTOCK.COM

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

BY MICHAEL LEWIS

DON'T MISS THE FOREST FOR THE TREES

Auditors who focus on findings misunderstand the purpose of their work.

Findings, observations, opportunities for improvement—regardless of the term used, some auditors define themselves by how many they can produce on each audit. Even experienced auditors often are reluctant to issue audit reports without this information, with some going out of their way to find at least something to include, even if it's trivial. But these practitioners are missing the forest for the trees. The errors or omissions identified during an audit should not be the focus of our work. Instead, auditors should fix their attention on what those errors say about the effectiveness of underlying controls and the strength of the overall control environment.

Internal auditors are responsible for assessing internal controls that contribute to the accomplishment of organizational objectives. According to The IIA's Definition of Internal Auditing, internal auditors do this by "bringing a systematic and disciplined approach to evaluate and improve the controls of the organization." Well-designed, operationally effective internal controls result in a higher likelihood that organizational objectives will be met.

Manual controls will always produce errors, regardless of how well they are designed, because of the human factor involved in their execution. Internal auditors should bear this in mind when encountering isolated or minor errors. Of course, higher-than-expected error rates could indicate that controls are not operating as effectively as intended—either because they are poorly designed, or the person performing them needs additional training. Manual control activities are performed by employees trained to carry out this function and therefore tend to be the source of many control failures. And because controls can be designed as preventive or detective, errors and omissions identified during an audit are those for which either there were no preventive controls in place or the preventive controls were ineffective. That should be the auditors' focus, not the errors themselves.

Internal auditors risk losing credibility with their primary stakeholders, and any hope of becoming their trusted advisor, when they consistently report on trivial issues that could be addressed outside of a formal audit report. If the impact of the audit observation does not pass the "so what?" test, it should not be included in the report. Ultimately, the audit committee wants to know that management is on track to meet its objectives—information on the effectiveness of the internal control system provides that assurance. If auditors are not speaking to the board and audit committee about the effectiveness of that system, they are not fulfilling their responsibility to their primary stakeholders.

The errors, omissions, or areas of noncompliance that auditors detect when reviewing transactions are not an end in themselves; they are the means to an end. When engagements are performed correctly, the end consists of providing information that both management and the board can use to increase their effectiveness and better position the organization for success. Ia

MICHAEL LEWIS, CIA, CISA, *is a senior internal auditor at Cru in Orlando, Fla.*

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