RISK IN FOCUS
A Survey of the Global Business Landscape

AN AUDIT OF KNOWLEDGE
Protecting a Company's Intellectual Capital

A STATE OF RESILIENCE
Resourcefulness in the Face of Disruption

internal auditor

DECEMBER 2023
A PUBLICATION OF THE IIA

The Analytics Advantage

Advanced technologies are helping auditors find fraud deeply hidden within their organizations.

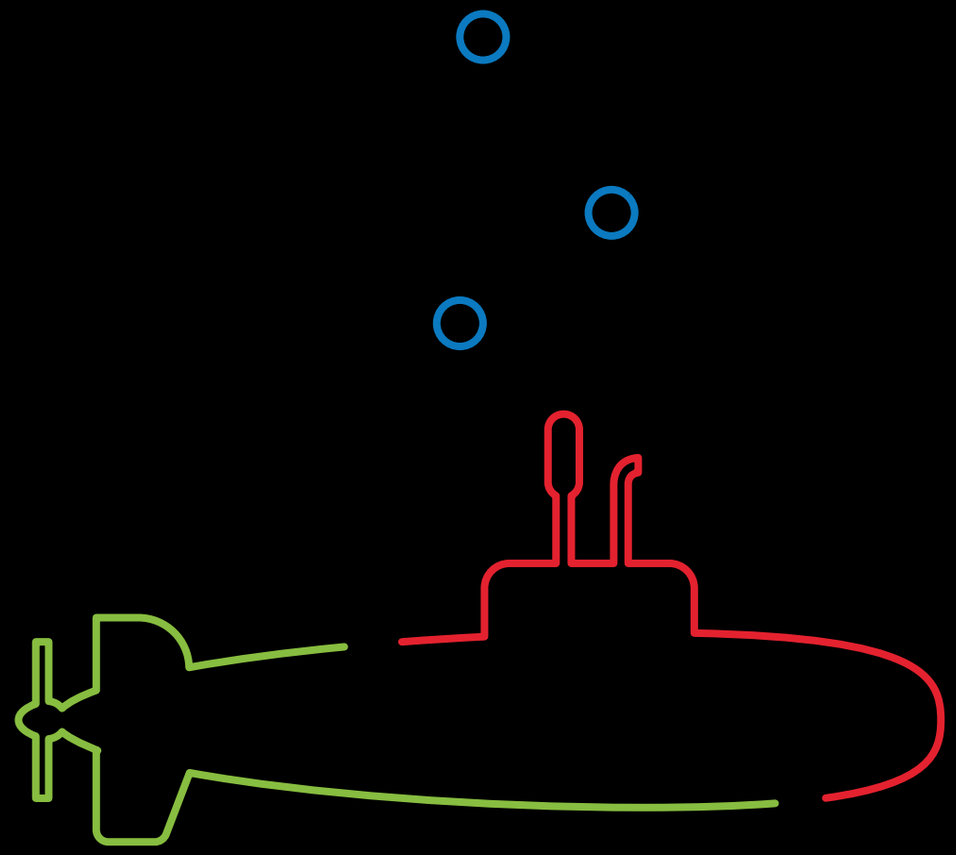
pwc

Global Internal Audit Study 2023

Seeing through walls to find new horizons

Wolters Kluwer

Dive deeper than dashboards.



TeamMate® helps auditors see more.

Is your dashboard all flash or does it let you see what's below the surface?
To find unknown risks you need to dive deeper.

Drill down on your dashboard data
Whether your audit committee is looking for greater insight into risks or audit performances, or auditors need a detailed list of their priorities, TeamMate will help you dive deeper.

See more than one dimension
TeamMate is the purpose-built audit solution with multi-dimensional reporting. Ensure your view of risk isn't limited by your audit management tool.

Find hidden insights
With an Excel-driven data analytics tool, a library of more than 150 tests, and features like the ability to visualize data to identify risks, TeamMate puts audit analytics in auditors' hands.

tm.wolterskluwer.com

needs
ROI
for
ESG

coffee:
black

500+
employees

we speak

CEO, straight talk and Susan

At Grant Thornton, we take the time to understand your challenges. Because, for us, it's about more than getting the job done—we get you.

Grant Thornton | Audit | Tax | Advisory | gt.com

contents

Featuring

35

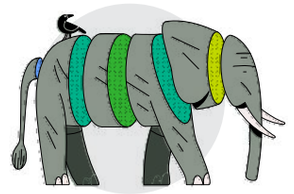
The Analytics Advantage

Advanced technologies enable internal audit to detect fraud deeply hidden within the organization. These analytics tools create a more dynamic, precise, and proactive way to identify deceptions.

Emily Primeaux James Grover

contents

Featuring



contents

Practices

contents

Insights

Connect Risk. Connect Your Teams.

THE MODERN CONNECTED RISK PLATFORM

AuditBoard helps you bring people, risks, and insights together to keep pace with today's demands and improve business resilience.

TOP-RATED AUDIT SOFTWARE ON

Gartner peerinsights ★★★★★

g2.com ★★★★½

Capterra ★★★★½

ceo message

Battling Fraud With Analytics

As we approach the end of another remarkable year, I'm filled with gratitude for the incredible dedication and resilience exhibited by internal auditors around the globe. Our profession's work has never been more important. The challenges our organizations face grow in number and complexity every day — and internal audit is the organization's best defense.

In this issue of *Internal Auditor*, we shine a spotlight on a vital tool in our ongoing battle to identify and prevent fraud — analytics.

Let's take a moment to consider the staggering costs of fraud. According to the Association of Certified Fraud Examiners, fraud losses account for approximately 5% of annual revenues worldwide. This translates to more than $4.7 trillion lost to fraud globally each year. These statistics underscore both the stakes and the urgency of internal audit's work.

And with a massive expansion of data to sort through, the job is getting tougher. According to International Data Corp., the world's data is expected to grow to a whopping 175 zettabytes (that's 175 followed by 21 zeros) by 2025.

This exponential growth in data presents a formidable challenge when it comes to uncovering fraud. Relying solely on internal controls is no longer sufficient in this data-rich landscape. Thankfully, data analytics software has emerged as a powerful ally in the battle.

Data analytics allow internal auditors to identify trends, patterns, anomalies, and exceptions within data — unveiling the digital fingerprints of fraudsters. It is imperative we not only educate ourselves on how best to use this technology, but also ensure our organizations invest in harnessing the transformative power of fraud analytics. As the opportunities for fraud grow, our defensive measures must keep pace so we can prevent its devastating impacts.

Internal auditors have numerous tools at their disposal to combat fraud, including: descriptive analytics, predictive analytics, prescriptive analytics, behavioral analytics, identity verification, real-time monitoring and detection, network analysis, machine learning and artificial intelligence, rules-based systems, visual analytics, text analytics, and big data analytics. Regardless of the tools we choose, the message is clear: We must use all available resources at our disposal to safeguard our organizations from fraud.

Anthony Pugliese

internal auditor

December 2023

Published by

The Institute of **Internal Auditors**

IIA President and CEO
Anthony Pugliese, CIA, CPA, CGMA, CITP

IIA Chair of the Board
Sally-Anne Pitt, CIA, CGAP

Editor in Chief
Anne Millage

Managing Editor
Tim McCollum

Senior Editor
Christine Janesko

Assistant Editor
Trinity Curbelo

Staff Writer
Logan Wamsley

Art Direction
Em Agency

Contributing Editors
Wade Cassels, CIA, CCSA, CRMA, CFE
Steve Mar, CFSA, CISA
Grant Wahlstrom, CIA, CPA, CFE
James Roth, PHD, CIA, CCSA, CRMA
David Dominguez CIA, CRMA, CPA, CFE

Social Media
@TheInstituteOf InternalAuditors
@TheInstituteOf InternalAuditorsInc.
@theiia

Advertising
advertise@theiia.org
+1-407-937-1109

Subscriptions, Change of Email Address
customerrelations@theiia.org
+1-407-937-1111

Editorial
Tim McCollum
tim.mccollum@theiia.org
+1-407-937-1265

Permissions and Reprints
copyright@theiia.org

Writer's Guidelines
internalauditor.theiia.org

Internal Auditor ISSN 0020-5745 is published in February, April, June, August, October, and December. Yearly subscription rate: $60. No refunds on cancellations. Editorial and advertising office: 1035 Greenwood Blvd., Suite 401, Lake Mary, FL, 32746, U.S.A.

Change of email address notices and subscriptions should be directed to IIA Customer Relations, +1-407-937-1111.

Statement of Ownership, Management, & Circulation

Extent & Nature of Circulation	Avg. No. Copies (11/2022-10/2023)	Actual No. Copies (10/2023)
Total Number of Copies	0	0
Paid Circulation Mailed Outside-County Paid Subscription	0	0
Paid Distribution Outside the Mail Including Sales, Through Dealers and Carriers, Street Vendors, Counter Sales, and Other Paid Distribution Outside USPS	0	0
Total Paid Distribution	0	0
Free or Nominal Rate Copies Mailed at Other Classes Through the USPS	0	0
Free or Nominal Rate Distribution Outside the Mail (Carriers or other means)	0	0
Total Free or Nominal Rate Distribution	0	0
Total Distribution	0	0
Copies Not Distributed	0	0
Total	0	0
Percent Paid	100%	100%
Paid Electronic Copies	101,913	102,346
Total Paid Print Copies + Paid Electronic Copies	101,913	102,346
Total Print Distribution + Paid Electronic Copies	101,913	102,346

Publication Title: Internal Auditor
Publication Number: 266-580
Filing Date: 10-19-2023
Issue Frequency: Bi-Monthly
Number of Issues Published Annually: 6
Annual Subscription Price: $60
Mailing Address of Known Office of Publication: The Institute of Internal Auditors, 1035 Greenwood Blvd., Suite 401, Lake Mary, Seminole County, FL 32746
Address of Headquarters: The Institute of Internal Auditors, 1035 Greenwood Blvd., Suite 401, Lake Mary, Seminole County, FL 32746
Contact Person: Anne Millage / 407-937-1234
Publisher: Jonathan Niebch, vice president of Global Marketing, The Institute of Internal Auditors, 1035 Greenwood Blvd., Suite 401, Lake Mary, FL 32746
Editor: Anne Millage, The Institute of Internal Auditors, 1035 Greenwood Blvd., Suite 401, Lake Mary, FL 32746
Managing Editor: Tim McCollum, The Institute of Internal Auditors, 1035 Greenwood Blvd., Suite 401, Lake Mary, FL 32746
Owner: The Institute of Internal Auditors, Inc.,1035 Greenwood Blvd., Suite 401, Lake Mary, FL 32746
Issue Date for Circulation Data: November 2022 - October 2023/October 2023
Signature and Title: Anne Millage, Editor in Chief, 10-18-23

editor's note

Don't Blink

And just like that, we say goodbye to 2023 — and to my 23rd year at The IIA. How can that be? When I moved to Florida all those years ago to assume the managing editor role, my daughter was five years old. She's getting married in 2024. I'm not crying; you're crying.

Time flies, as they say. *Internal Auditor* will celebrate its 80th anniversary next year. When I started with The Institute, the magazine was a print publication only. As the Internet came into play, we introduced a magazine website to accompany the print publication. Next came the digital magazine.

In 2020, during COVID-19, we printed *Internal Auditor* for the last time, and in 2022, as part of The IIA's digital transformation, the publication became a redesigned-for-digital magazine. And, beginning with the October issue, the digital magazine is on a new, more visual, user-friendly platform. Make sure you check it out — maybe have it read you an article.

However, the reports of print's death have been greatly exaggerated. We've heard from members that they miss the print publication — holding it in their hands and flipping through the pages. So... North American members should look for a print version of the February 2024 issue of *Internal Auditor*!

The February issue will be a special one, as we introduce The IIA's Global Internal Audit Standards. We will delve into what's new in the Standards, take a deep dive into the five domains, consider how to apply the Standards in internal audit's daily work, and share the changes in governance expectations introduced in them.

We also are looking at printing the August issue, which will celebrate the magazine's anniversary, and will consider additional print editions in 2025.

Internal Auditor has continuously evolved over its 80-year history, always to better meet our readers' needs. With a new digital platform and two print issues, we're looking forward to continuing that evolution in 2024.

Anne Millage

Crowe | The Institute of Internal Auditors

Internal auditors AI safety checklist

Are you using AI safely?
5 questions to know for sure.

AI can help internal auditors demonstrate more value in less time, but it's critical to understand the risks and rewards that come with it.

Use this checklist as a tool to help determine if you're using AI safely and effectively.

Download now

update

Technology Risk Levels Rising

CAEs and IT auditors weigh tech risks in a new global survey.

Today, the risk landscape is evolving at an accelerated rate, creating more opportunities than ever for internal audit to enhance its organizational value. Nowhere is this truer than in the realm of technology, where risk areas such as cybersecurity and artificial intelligence (AI) continue to become more central to organizational focus.

This is one of the key findings from the 11th annual Global Technology Audit Risks Survey from The IIA and Protiviti. Using feedback from over 550 CAEs and IT audit professionals received earlier this year, the survey explores the top technology risks companies are facing over the short-term (12 months) and medium-term (up to three years). It also explores the practices, processes, and tools used by organizational functions to identify, manage, and mitigate these risks.

"Risks related to cyber and AI look radically different than a few years ago and will surely continue to evolve," says Angelo Poulikakos, global leader of Protiviti's Technology Audit and Advisory practice. "Companies that conduct internal audits more frequently and integrate advanced analytical tools and techniques into their audit processes will be more on top of these changes and consequently more prepared when real issues arise."

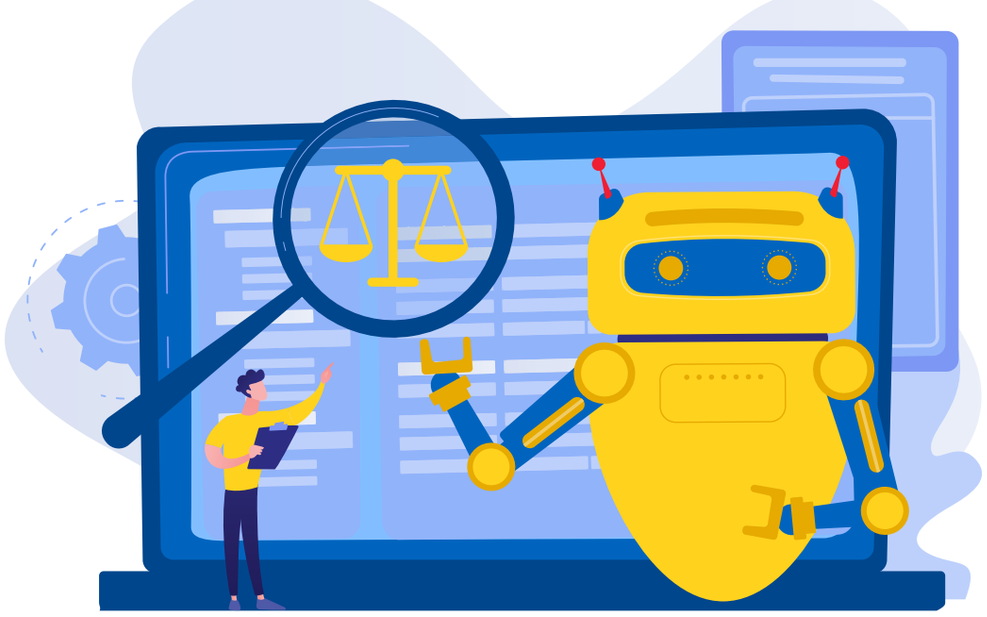
According to the survey, CAEs and IT audit leaders are well aware of the technology challenges ahead. For example, 74% of respondents consider cybersecurity to be a high-risk area over the next 12 months. Among CAEs, that number grows even higher to 82%.

Other technology risks, while having a relatively low perceived risk level short-term, are expected by audit leaders to emerge in the coming years. AI is a primary example of this, as only 28% of respondents indicate that AI and machine learning will be a significant threat in the next 12 months. However, in the next two to three years, that figure rises to 54%. **—Logan Wamsley**

ADJUSTING TO A CARBON TARIFF

"CBAM is expected to drive up the prices of regulated products and prompt customers to take a second look at suppliers." **—Anuj Saush, leader, Environmental, Social & Governance Center, Europe, The Conference Board, on the Carbon Border Adjustment Mechanism (CBAM).**

SOURCE: THE CONFERENCE BOARD, CEO INSIGHT MINUTE: WHAT SHOULD BUSINESS KNOW ABOUT EUROPE'S CARBON TARIFF?



Putting Guardrails on AI

Leaders in responsible AI collaborate to create a governance framework.

Some of the biggest corporate thinkers on AI have teamed up for a new white paper on creating an AI governance framework. An Insider's Guide to Designing and Operationalizing a Responsible AI Framework, published by EqualAI, was coauthored by executives from Amazon Web Services, Google DeepMind, LivePerson, Microsoft Corp., Northrop Grumman Corp., PepsiCo Inc., SAS Institute, Salesforce Inc., and Verizon.

The report gives guidance on how to establish and implement responsible AI governance, according to EqualAI, a nonprofit focused on reducing unconscious bias and other risks in the development and use of AI.

"The reality is that nearly every company is a technology company today," said Catherine Goetz, global head of Inclusion Strategy at LivePerson, in an Equal AI podcast. "The white paper does such a good job of mapping out step-by-step of how an organization can get started [in AI governance]."

The report details 11 principles that are critical to adopting an AI system and setting up governance. These include the preservation of privacy, transparency, a human-oriented focus, respect for individual rights and societal good, open innovation, rewarding robustness, continuous innovation and review, employee involvement, prioritizing fairness through accountability, ongoing human oversight, and professional development.

It also introduces six central pillars needed for responsible AI frameworks: responsible AI values and principles; accountability and clear lines of responsibility; documentation; defined processes; multistakeholder reviews; and metrics, monitoring, and reevaluation.

In a press release, EqualAI urges organizations not to wait to adopt best practices for AI governance. "The potential harm and liability associated with the complex AI systems currently being built, acquired, and integrated is too significant to delay."

The white paper preceded U.S. President Biden's executive order on AI, which was released in October. The order focuses on transparency, testing, cybersecurity, safety, and data protection.

—Christine Janesko

WHY YOUNG PEOPLE MOVE ON

Top priorities of Millennial and Gen Z adults considering a switch to a new employer:

68% Compensation

50% Opportunities for promotion and growth

49% Flexible work schedule

39% Quality of benefits

SOURCE: GEORGETOWN UNIVERSITY AND BANK OF AMERICA, YOUNG ADULTS AND WORKPLACE WELLNESS

ASK AN EXPERT

The DOJ Levels Up

Scott Boylan, former U.S. DOJ attorney and Homeland Security advisor, is a partner at StoneTurn, and is based in Washington D.C.

How is the U.S. Department of Justice targeting corporate crimes involving national security?

The National Security Division at DOJ has recently announced the appointment of a chief counsel for corporate enforcement and the hiring of dozens of prosecutors to investigate and prosecute bad corporate behavior relevant to national security. Areas likely to be impacted are export control, sanctions, and enforcing agreements that companies have with the Committee on Foreign Investment in the U.S. (CFIUS), for example.

We will see a significant increase in prosecutions of companies in these and related areas, similar to what happened with the Foreign Corrupt Practices Act (FCPA). When I was at the DOJ Criminal Division decades ago, the FCPA office was tiny, and the attorneys assigned to it spent most of their time educating corporations on the requirements of the law and encouraging compliance programs. That changed in the early 2000s when the Bush Administration increased resources for FCPA investigations and prosecutions skyrocketed. I expect the same to occur with national security prosecutions.

What steps can organizations take to stay in compliance?

Companies need to evaluate their compliance regimes with a national security lens. They should be especially vigilant when conducting due diligence during acquisitions. Companies will need to have clear guidance on self-disclosing issues related to national security in the M&A process, or subject themselves to potential criminal liability.

I believe this will cause an escalation in the enforcement of CFIUS and similar mitigation agreements. CFIUS has already gotten more aggressive in fining companies. Now companies and individual employees responsible for enforcing mitigation agreements could find themselves being prosecuted for violating those agreements.

EASY TARGETS

U.S. bank customers who experienced some form of bank fraud in 2022 and 2023:

50%
OF PEOPLE DESCRIBED AS FINANCIALLY OVEREXTENDED

47%
OF PEOPLE UNDER 40

35%
OF BANK CUSTOMERS OVERALL

SOURCE: J.D. POWER, BANKING AND PAYMENTS INTELLIGENCE REPORT

Awash in Misleading ESG Claims

Greenwashing and social washing were on the rise in 2023.

70%
increase in climate-related greenwashing incidents in the financial services industry

15%
increase in social washing incidents overall

31%
of publicly listed companies linked to greenwashing also are associated with social washing

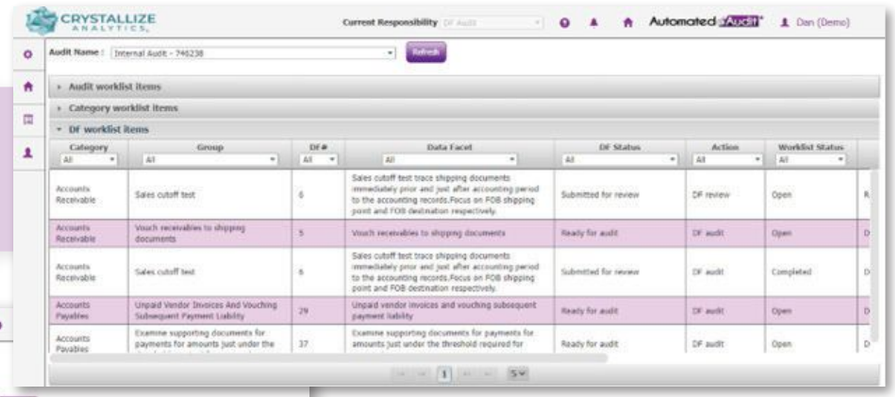
SOURCE: REPRISK, ON THE RISE: NAVIGATING THE WAVE OF GREENWASHING AND SOCIAL WASHING

Automated $Audit®

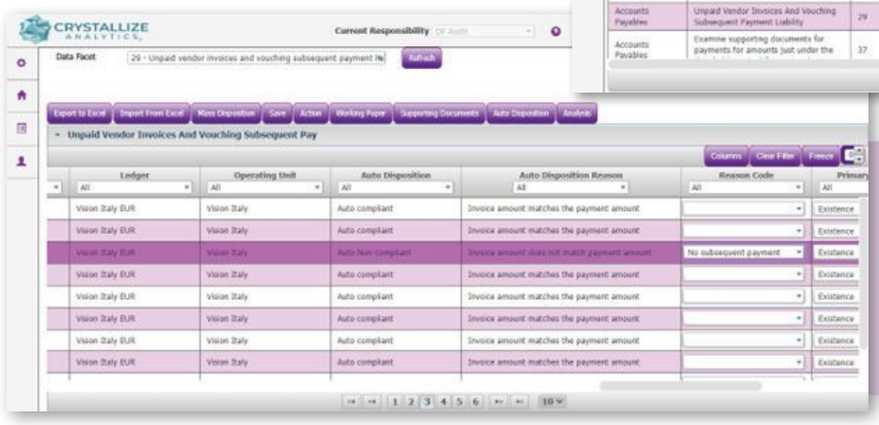
Your audit processes, empowered.

Automated Audit® software provides auditors and finance teams with streamlined data and standard procedures, enabling companies to gain valuable insight and confidence in preparation for their financial audit.

By accessing complete and accurate data directly from the ERP database, Automated Audit offers finance teams unparalleled visibility and oversight. Leveraging the software's signature Data Facets™ (automated validation activities) auditors of any experience level can easily identify issues or differences, such as material misstatement or fraud at the assertion level, to correct discrepancies prior to the audit. Streamline your audit processes and set your organization up for audit success.



Easily configure each Data Facet and working paper to show only the data that you want to see.



Automated Audits' Auto Disposition handles the heavy lifting, identifying indicators of non-compliance in plain language so auditors can focus on investigating issues rather than finding them.

Automated Audit works by first extracting and assembling ERP data, eliminating the need for IT requests, cleaning, formatting, or analyzing flat files. Next the software presents findings, with interactive visuals, so that auditors can easily identify differences and anomalies. The software's built-in Data Facets then incorporate logic to identify items or transactions of concern using the auto-disposition feature. Your team of auditors then can review the data and determine compliance either entry by entry, or in bulk with a mass disposition tool, or utilizing their favorite tools, such as Microsoft Excel. Once your team has completed their due diligence, Automated Audit generates documentation such as working papers, lead schedules, and audit reports to document the auditors' findings.

Benefit Overview

- ✓ All transactions and balances included in your audits are validated to the trial balance ensuring completeness of data with the ability to drill down to individual transactions and roll up to summary balances for each company.
- ✓ Allows manual, time-consuming audit activities to be automated and carried out by no-code-needed substantive procedure Data Facets
  - Connection to ERP by direct access to the database
    - No creation of extracts or loading files into software
    - Potential for 100% transaction and balance coverage-elimination of sampling with the accompanying Type I, Type 2, and error extrapolation risks
    - Audits the entire population of the data for the selected financial period(s)
      - Pulls transactions of different types, methods, and technology stacks into the product layer when analyzing/reviewing a specific transaction.
- ✓ Analytics software products that automate the financial audit and provide ongoing fraud detection, cost recovery, and operational improvement with built-in intelligence including auto-disposition to detect anomalies and potential misstatements with visualizations to provide unique insights into your data.

- ✓ Bridges skill gaps and resource constraints
  - Streamline tedious manual tasks to save time and money and let your skilled professionals focus on areas of compliance and analysis that best serve the business's forward momentum and conform to your audit plan.

Schedule a demo today.

www.crystallizeanalytics.com

basics

5 Traits of Great Auditors

Successful practitioners share these core attributes.

Marie C. Dunbar

My journey to internal auditing was not a planned one. Instead, I stumbled upon it. Like many other internal auditors, I started on a different career path. After majoring in marketing, I got my first job in customer service and copy editing. My various supervisors and mentors saw something in me that at the time I did not: They recognized an aptitude for quickly picking things up and analyzing.

At one point, my supervisor made me responsible for reviewing and clearing billing discrepancies on customer accounts. After mastering this task, I was promoted to a controller-oriented function where I performed daily account reconciliations and ensured accurate ledger and subledger bookings.

Over time, a few internal audit tasks made their way into my work, which included keeping records accurate and controls tight to meet business needs. Through these assignments, I developed an affinity for the work. As a result, I began researching internal auditing, along with the skills needed to succeed in the profession. Eventually, I leveraged my experiences to make a career change.

Four years later, I am a Certified Internal Auditor, have a Certification in Risk Management Assurance, and have learned the core attributes necessary to becoming a professional internal auditor.

Keys to Success

All internal auditors must have certain skills and knowledge to grow in their careers. They must be analytical, focused, people-oriented, and able to clearly communicate. To the same degree, auditors should possess traits such as curiosity, integrity, and the ability to practice confidentiality. Through my experiences, I have identified five core features of successful internal auditors.

1. Be an Excellent Communicator. The ability to communicate well can determine an internal auditor's success in the profession. Auditors constantly interact with stakeholders and process owners. They must be able to navigate these relationships and sometimes bridge conflicting views on what is important and aligns with organizational goals.

Communication skills include both verbal and written proficiency. My earlier customer service and communication roles proved helpful in improving my verbal skills. I have found listening, asking the right questions, and speaking concisely beneficial to getting my point across during my various interactions.

As for writing proficiency, auditors must concisely communicate audit findings, discuss potential risks, and recommend improvements in audit reports. Following grammatical rules and proofreading before issuing any communications builds a practitioner's credibility as a competent auditor. It is imperative to know the target audience and tailor the message accordingly so the audit experience and recommendations for improvement are maximized.

Depending on the stakeholder being addressed, the goal may be different. Hence, knowing how to leverage the "what's in it for me?" helps create that customer connection and can sooth the engagement process.

2. Be Curious. Great auditors have an inquisitive mind. They don't take things

at face value. Great auditors continually ask questions until they fully understand the issue at hand. Professional skepticism is a well-known term in the internal audit world and is helpful in detecting fraud, financial misstatements, and other wrongdoing.

With a focus on the "why" throughout root-cause analysis, great auditors keep digging until they find the answers they are seeking.

3. Be Passionate About Learning. The profession encourages continuous learning. To stay up to date with the various standards, accounting, and state regulations, many certifications require continuing professional education (CPE) hours on a yearly basis. Obtaining CPE hours satisfies one of The IIA's Code of Ethics Rules of Conduct for Competency, which states that internal auditors should continually improve their proficiency and the effectiveness and quality of their services.

One of the benefits of the profession is that no audits are ever the same. Internal auditors get to experience many different parts of the organization. However, without the willingness to learn, it will be challenging to approach each assignment. Being able to quickly absorb information and learn additional parts of the business can improve auditors' chances to succeed.

Having a diverse set of skills and training can make auditors more attractive to employers, more comfortable, and better at resolving the issues they encounter in their daily work. Auditors beginning their internal audit careers should take advantage of IIA conferences, *Internal Auditor* magazine articles, and webinars from The IIA and its partners.

4. Be Ethical. Integrity is another principle of The IIA's Code of Ethics: "The integrity of internal auditors establishes trust and thus provides the basis for reliance on their judgment." According to the Rules of Conduct, auditors are expected to perform their work with honesty, diligence, and responsibility. This entails observing the law, following the *International Standards for the Professional Practice of Internal Auditing*, and reporting any identified deficiencies.

There may be instances when auditors are asked to look the other way or ignore a faulty control or management override, yet they must do the right thing. It's never easy to confront and bring to light someone who is being unethical, but good auditors are never swayed.

5. Be Trustworthy. Auditors should be careful in the use and protection of information acquired in the course of their work. As the Code of Ethics states, internal auditors should not "disclose information without appropriate authority unless there is a legal or professional obligation to do so." Moreover, auditors must refrain from using information for personal gain or in any way that would be contrary to the law or the *Standards* or detrimental to the legitimate and ethical objective of the organization.

It's never easy to confront and bring to light someone who is being unethical, but good auditors are never swayed.

The Path to Greatness

Working toward improving in these five areas will help auditors excel in the profession. The list is not exhaustive, or a one-stop shop to rise through the ranks in internal auditing. But focusing on these as a starting point can help internal auditors get on the right track to success. As auditors embark on their professional quest, they will have to overcome a learning curve and many challenges. By understanding these fundamental skills and the Code of Ethics of this profession, auditors are better equipped to perfect their craft.

Marie C. Dunbar, CIA, CRMA, AMLCA, is a senior business analyst at NextEra Energy Resources in West Palm Beach, Fla.

tech

The Security Interchange

While cybersecurity protects the world's digital roads, information security safeguards the information traveling along them.

Antonio Magallanes-Villamor, Jr.

Internal auditors may feel overwhelmed when tasked with providing assurance or advice on organizational information security or cybersecurity. Distinguishing between these two fields can be perplexing. As a result, many internal audit, assurance, and IT professionals are confused about the differences between cybersecurity and information security and the risk areas each considers.

In reality, the core aspects of cybersecurity and information security are the same — both aim to protect data and information while preserving confidentiality, integrity, and availability. One concerns digital roads, while the other concerns traffic. Rather than reflecting on their

differences, auditors should focus on what they have in common.

Defining Cybersecurity

One reason for this confusion is that cybersecurity does not have a uniform definition. For example, the U.S. National Institute of Standards and Technology defines *cybersecurity* in several ways, including:

- The ability to defend the use of cyberspace from cyberattacks.
- A process of preventing, detecting, and responding to attacks to protect information.
- Preventing and protecting against computer damage, electronic communications systems and services, and wire communications.

Formal definitions aside, cybersecurity encompasses interactions among people, systems, knowledge, networks, devices, instruments, and programs used within and around an organization's network and the broader cyberspace. These interactions create dependencies among networks of information system infrastructure, telecommunications networks, computer systems, and embedded processors and controllers. All these components require protection from cyber threats that come from both the internet and inappropriate or malicious system usage. Cyber threats become institutional and national security risks when they threaten a nation's critical infrastructure.

Cybersecurity also is a professional field with several branches, including privacy. Cybersecurity experts are particularly concerned with security issues arising from the significant increase of data. Recently, there has been growing concern that artificial intelligence can be used to develop more sophisticated attacks that replicate human behavior and target low-level systems.

Beyond technology, professions such as psychology, assurance, management, international relations, public policy, physics, and engineering all are involved in research, policy development, and technology improvements to address cybersecurity challenges. Within organizations, it is a concern for IT, audit, risk management, legal, human resources, communications, and physical security teams.

Securing Information

Information security is concerned with protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction. Specifically, it focuses on the confidentiality, integrity, and availability of systems or procedures that collect, organize, and disseminate information.

Confidentiality is about ensuring that only authorized people and processes can access information. Integrity is about preventing an unauthorized person or process from altering information regardless of its state (i.e., at rest, in transit, or in use). Availability means that authorized personnel or processes can access information whenever needed.

Effective information security demonstrates that an organization has sound information resource management. That requires organizations to have resources, governance, risk management, compliance, and control measures in place to achieve their information security goals.

Moreover, all organizations contributing to the information ecosystem must have effective information security mechanisms to be credible and trusted parties in cyberspace. They should ensure that their information systems and resources are free from potential exploits and would not serve as a source of cyber threats for organizations they interact with online.

To become more resilient, organizations can take measures such as implementing firewalls, intrusion detection systems, encryption, and access controls. They also should put in place secure communication protocols, encrypted data transmission, and secure payment gateways to protect sensitive information. Failure to implement information security rules and procedures can negatively impact an organization's ability to conduct business over the internet.

Effective information security demonstrates that an organization has sound information resource management.

It's About Protecting Information

At their core, both information security and cybersecurity are concerned with protecting information. Information is a powerful tool that individuals, institutions, and societies use for decision-making and influencing

actions. Information and its supply chain should be protected in a hyper-connected world with highly complex information systems. Otherwise, they can be weaponized by people and organizations with harmful intentions.

In March, the European Network and Information Security Agency listed 10 emerging cybersecurity threats and challenges for 2030:

1. Supply chain compromise of software dependencies.
2. Advanced disinformation and influence operations campaigns.
3. Digital surveillance authoritarianism and loss of privacy.
4. Human error and exploited legacy systems.
5. Targeted attacks, such as ransomware, enhanced by smart device data.
6. Lack of analysis and control of space-based infrastructure and objects.
7. Advanced hybrid threats.
8. Skills shortages.
9. Cross-border information and communications technology service providers as a single point of failure.
10. Abuse of AI.

Both information security and cybersecurity threats involve data and information, such as inserting back doors in open-source libraries, identity spoofing, manipulating access to national services, analyzing legacy operational technology equipment for vulnerabilities, and using AI to analyze data from smart devices. Attackers may access space infrastructure to create malfunctions or malware to sabotage other governments, disrupt critical infrastructure, and leverage user and behavior analytics to sow discord. Threat actors can even use public job ads to learn about an organization's skill gaps and outdated systems.

In response, organizations adopt technology tools to protect data and information confidentiality, integrity, and availability. These tools constantly change in response to many factors, such as the need to innovate and become more efficient in resource use as science and engineering evolve. The tools also must keep up with advances and challenges posed by threat actors. Internal auditors' appreciation of these developments should progress as technology advances.

Information security and cybersecurity require organizations to manage future risks and respond to current and past incidents. It requires hindsight, insight, and foresight into vulnerabilities and how to prevent or reduce them, including the probabilities of a threat, the costs associated with potential outcomes, and how to mitigate them. Internal auditors should not be intimidated by risks associated with technological advances.

Converging Roads

Cybersecurity and information security are essential for protecting data and information. Cybersecurity covers anything and everything in cyberspace, while information security applies to all information wherever it is located. With subtle distinctions, these fields overlap and share many standards, best practices, and control measures.

To feel confident, internal auditors must understand the technologies their organizations have adopted when providing assurance or advice. After all, the goal of information security and cybersecurity is safeguarding the organization's data and information.

Antonio Magallanes-Villamor, Jr., CIA, CRMA, CISA, CISM, is head of the Internal Audit Unit at the International Center for Agricultural Research in the Dry Areas based in Cairo.

Cybersecurity and information security are essential for protecting data and information. Cybersecurity covers anything and everything in cyberspace, while information security applies to all information wherever it is located.

WHAT'S ESG GOT TO DO WITH FRAUD?

The unscrupulous are finding ways to misrepresent company practices.

Environmental, social, and governance (ESG) has gained significant traction in the business world over the last few years. As investors and other stakeholders embrace ESG by channeling investments and other support to companies with strong ESG commitments and performance, sustainability, diversity, equality, and governance criteria have become essential data points as stakeholders seek to make informed investment and purchasing decisions.

Those stakeholders currently rely on voluntary sustainability reports that use one of many ESG frameworks and generally are without the benefit of third-party assurance attesting to the integrity of the disclosures. This less mature environment creates a situation where the unscrupulous can defraud others by intentionally manipulating, misrepresenting, or concealing information related to a company's ESG practices.

To provide context and better understand what is happening with ESG fraud, here is a recap of a few conversations we've had recently with internal auditors.

CAN YOU PROVIDE A FEW EXAMPLES OF ESG FRAUD?

- **Greenwashing:** Intentionally exaggerating or fabricating environmental credentials, including misleading claims about reduced carbon emissions, renewable energy usage, and sustainable sourcing, without appropriate substantiation.
- **Social Impact Inflation:** Inflating or misrepresenting a company's social impact, such as contributions to local communities, diversity and inclusion initiatives, or employee well-being programs, and creating a false perception of its commitment to social responsibility.
- **Governance Manipulation:** Deceiving stakeholders in areas such as internal control structures, executive compensation, and compliance practices.

WHAT ARE SOME WAYS COMPANIES MONETIZE THESE FRAUD SCHEMES?

- **Supply Chain:** Inflating their ESG credentials can help companies retain existing or attract new customers who incorporate ESG metrics into their selection criteria.
- **Access to Capital:** Whether by misleading investors by exaggerating ESG metrics to increase the company's share price, or by misrepresenting ESG data to obtain preferred interest rates or less stringent loan covenants from a lender, companies can gain access to cheaper capital to fund their operations.

WHAT TYPES OF IMPACTS CAN ESG FRAUD HAVE ON STAKEHOLDERS?

ESG fraud can lead to significant financial losses for investors or lenders who need accurate and reliable financial and ESG information for their investment decisions. Misleading disclosures can artificially inflate stock prices and misdirect capital, resulting in substantial financial harm.

Companies found guilty of ESG fraud may experience fines and penalties, plus severe reputational damage. Trust among stakeholders, including customers, employees, and investors, can be eroded, leading to long-term consequences for the company's brand value and market position.

ESG frauds undermine the broader goals of sustainability and responsible business practices. They create skepticism and cynicism in the marketplace and can cause a misallocation of capital and hinder efforts by stakeholders to support climate change, social equality, and other efforts.

WHAT STEPS ARE BEING TAKEN TO COMBAT ESG FRAUD?

Regulators are implementing disclosure and reporting requirements along with increased ESG reporting oversight and enforcement activities. A significant element of this regulatory shift is the adoption of assurance requirements for mandated ESG disclosures. Third-party assurance can help validate the accuracy and transparency of ESG assertions, reducing fraud risk.

Investors and creditors are demonstrating a "buyer beware" mentality by expanding their ESG due diligence activities (including reviewing relevant documentation), conducting site visits, scrutinizing sustainability reports, and more. These efforts can identify red flags and potential instances of fraud.

Most auditors are familiar with the three elements of the fraud triangle: pressure, opportunity, and rationalization. So how does all this fit into that triangle?

As financial resources shift to entities that are focusing on reducing their environmental footprint and enhancing social equality, organizations that are not focusing on ESG can feel increased pressure to "prop up" their ESG metrics to maintain capital availability to operate and grow their business.

As is typical with frauds, a perpetrator's ability to interpret the situation as unjust or to over-index on real or perceived slights enables them to rationalize the fraudulent behavior — besides, "everybody's doing it," right?

WHAT ROLE DOES INTERNAL AUDIT HAVE IN ALL THIS?

Internal auditors generally can make the greatest impact by helping the organization reduce the opportunity for fraud and, thus, the likelihood of a significant fraud. Internal auditors do this by applying their expertise to identify and assess risks, deploy preventive and detective internal controls, encourage communication and information sharing, and evaluate the effectiveness of the program over time.

This is an incredible time to be an internal auditor; each of us has the opportunity to proactively mitigate ESG fraud risk. Will we rise to the occasion or let it pass us by?

Today's **Global Risk** Landscape

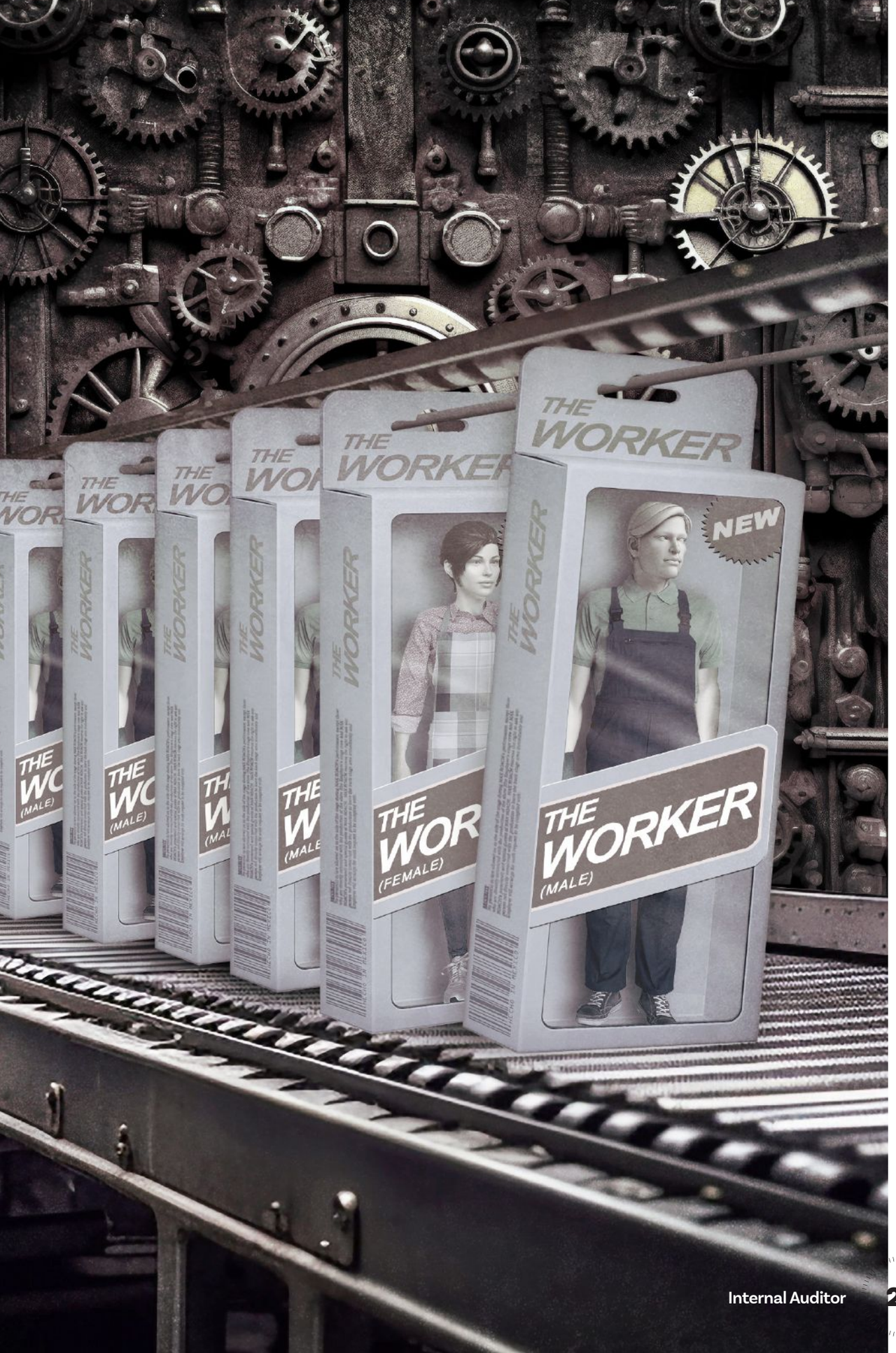
Around the corner and around the world.

Risk in Focus is a worldwide collaborative partnership facilitated by the Internal Audit Foundation. It provides practical, data-driven research to help internal auditors and their stakeholders understand today's risk environment and prepare audit plans for the year ahead.

HOT TOPICS FOR INTERNAL AUDITORS | BOARD BRIEFINGS | THEMED, REGIONAL REPORTS

Download Now
theiia.org/RiskInFocus

Internal Audit FOUNDATION



risk

The Exploited Worker

Organizations may be unaware of their exposure to labor abuse.

Maja Milosavljevic Joshua Clark

Most internal auditors would not think their company could be involved in labor exploitation. However, labor law violations could be occurring even when the underlying activities are legal.

Labor exploitation is the mistreatment of individuals in a work setting for profit. The abuse can take various forms, ranging from direct and brutal to something much less obvious. However, its impact can be detrimental to victims on psychological, physical, emotional, and financial levels. Examples range from low wages and poor working conditions to child labor and human trafficking.

Internal auditors should assess whether their organization is at risk of violating labor laws, as the consequences could be severe.

How Exploitation Happens

Today, companies often struggle to find enough personnel locally for various types of business activities. As a result, they often hire people from around the world for certain positions — both people who have already immigrated to the country and others who move there for the job. Depending on the work being performed, labor contracts may

Contractors may not be adequately paying their employees or treating them well. The contracting company might not even realize workers are being mistreated.

provide for housing, meals, and other benefits.

However, salaries, labor treatment, legal protections, and living conditions for these immigrant workers can be widely different in various regions of the world. Employees may believe they are being paid fairly compared to wages in their home countries even though their pay might be below the minimum wage of the country in which they work.

With companies that engage with foreign contractors for various activities, labor exploitation can be more complicated. Contractors often engage subcontractors, and those subcontractors may hire more subcontractors. Through this chain, these contractors may not be adequately paying their employees or treating them well. The contracting company might not even realize workers are being mistreated, yet it could be liable for such conditions.

What's at Risk?

Besides legal liability, another risk from labor exploitation is the damage to the company's reputation. Although this risk is difficult to quantify, the short-term compromise for profit over business ethics could lead to long-term consequences:

- Customers stop buying products or services.
- Potential employees do not want to work for the company.
- Financial institutions and investors discontinue their business relationships with the company.

If accused of violating labor laws, it is not enough for companies to claim that they did not know the exploitation was happening as this is "how it has always been." In fact, a response like this could be why a company failed to prevent or detect unfair labor practices.

Getting It Right

Internal audit can help the organization ensure it has appropriate labor practices.

Assess the tone at the top. Top management determines the ethical environment and serves as role models for employees. If top managers start to tolerate deviations or any kind of misconduct, the door for problems opens.

Internal audit should assess whether top management has established a strong corporate culture that includes adequate structures, processes, and controls to address labor exploitation risks. For example, internal audit should ensure executives and other management are aware of these risks, and it should assess whether the organization is able to respond adequately to potential issues.

Know the company's supply chain. Internal auditors can help the company assess the supply chain and provide assurance on how well it mitigates labor exploitation risks. Countries such as Germany and Switzerland have human rights laws in place that define requirements for responsible management of supply chains. Laws, directives, and regulations require adequate due diligence and, in certain instances, the need to report to authorities when illegal matters begin surfacing.

Assess supplier bids. Internal audit should evaluate bids from suppliers and consider every aspect of the offer, not just whether it is the lowest bid. Although auditors cannot be involved in selecting a supplier, they can audit the supplier selection process to ensure that all the relevant considerations are integrated into the process. In assessing the supplier qualification process, auditors should include the social criteria, in addition to technical or economic terms and evaluations.

In cases where a company awards contracts to the significantly lowest priced bid, this may indicate labor exploitation risk exposure, because the company may not pay its workers or may pay them lower than minimally required. Companies should assess and compare individual labor rates by categories based on workers' qualifications.

Assess supplier relationships. Internal audit also should examine how the organization manages its relationships with suppliers to ensure their labor conditions are receiving adequate attention. Auditors can do this by establishing dedicated channels for raising concerns about suppliers, maintaining an open relationship with suppliers, and being sensitive to information they receive about a supplier that may indicate a violation of labor law. Moreover, auditors should assess formal and informal communication channels between the company and suppliers.

Verify the controls to mitigate labor exploitation. To ensure controls are established and operating effectively, internal audit should conduct fieldwork to address the relevant matters in the vendor management process. Auditors should ask:

- Do the contractors' employees have the required visas and labor permits to work in a specific country/region?
- Do the salaries and wages the contractor pays comply with local laws and regulations?
- Does the contractor pay timely and regularly for the work done?
- Does the contractor provide employees with appropriate living accommodations, where required?
- Does the contractor care for the welfare of its employees?
- What are the rights and obligations of the company engaging contractors and subcontractors?

Auditors can seek answers to these questions in different ways. Their first step in auditing labor exploitation risk exposure should be verifying the legal options and restrictions that apply to the organization. Auditing suppliers is one option, if the audit is legally and contractually permitted.

To obtain the most reliable information, auditors should engage with contractors via interviews or observations and subcontractors' employees directly, and during on-site visits. However, the ability to make site visits may be impacted by travel budgets, the need to obtain visas and permits for audit team members, and language differences.

Assess the compliance and procurement functions. Auditors should assess how well these functions work together to mitigate labor exploitation risks. While the compliance department can provide a code of ethics for business partners, it must agree with procurement on which actions to take once the organization has identified inappropriate behavior. Because there can be various levels of inappropriate behavior, these two functions should consider a range of the possible actions to protect the interests of the company and find alternatives for business continuity.

Auditors can help compliance and procurement by providing advice on different options and approaches for assessing suppliers' risk and by explaining potential consequences in case of misbehavior.

The Long-term Impact

The relationship between profit and business ethics can be explained as a leverage effect. Although weak business ethics could result in higher profits in the short term, the long-term impact to the organization of such behavior could be extremely damaging. External stakeholders should evaluate every aspect of a business's behavior, including human rights. Internal audit can help defend the organization from labor exploitation risks by assessing the exposure and recommending improvements.

Although weak business ethics could result in higher profits in the short term, the long-term impact to the organization of such behavior could be extremely damaging.

Maja Milosavljevic, CIA, CRMA, CCSA, is a director of internal audit at Borealis in Vienna and a 2015 *Internal Auditor* Emerging Leader.

Great Audit Minds
Maximize Value

GAM is the premier event for internal audit innovators, leaders, and trailblazers to engage with each other on solving today's business and audit challenges and exploring tomorrow's new frontiers.

March 11-13 | ARIA Resort & Casino | Las Vegas, NV & Virtually
Members can save $580 on In-Person Registration
Register today at theiia.org/GAM

GAM Great Audit Minds
WHERE LEADERS EVOLVE.

fraud

Small Signs of Big Problems

The discovery of a forged signature leads to a much bigger fraud.

David Kirtland and Laura Harris Joshua Clark

Thomas Mooreland thought his eyes were playing tricks on him, but the more he looked at the two signatures, the more different they looked from each other. One signature had quick, bold strokes, whereas the other had a soft flow with the name slanting in a different direction. But in both signatures, the name was the same.

Mooreland, an internal auditor for PoGo, a technology company, noticed the discrepancy when he was reviewing transactions for the company's MindSweep subsidiary. PoGo had owned MindSweep for five years and used the computer hardware company to create supply chain efficiencies. Mooreland knew the company well enough that he was expecting to quickly check the books before moving on to another subsidiary.

However, during his review, Mooreland also noticed how much

MindSweep had spent on shipping. Although nothing was outwardly unusual, he wanted to take a closer look at the areas and numbers he normally audited, starting with MindSweep's packaging and shipping function.

Mooreland quickly discovered that MindSweep outsourced packaging and shipping to another company, PackRight, which was based in a country with a high-risk profile. While other tech companies had operations in that country, Mooreland knew it also was a common base for shell companies and other legally questionable business activities. With that in mind, he set out to investigate anything suspicious.

At first nothing seemed wrong: The paperwork checked out, the numbers reconciled, and the documents were accurate. That changed when Mooreland began seeing documents with different signatures for Evan Simms, MindSweep's chief logistics management officer. The documents included contracts, vendor approvals, and expense reports, and the signatures varied depending on the type of document Simms was signing. Mooreland suspected someone was forging Simms' signature.

If Mooreland was lucky, Simms would know who the forger was. Rather than calling Simms, he decided to document his actions with an email first, asking Simms to meet with him over the phone to discuss some questions that had arisen during the audit.

During their conversation, Simms attributed the discrepancy in the signatures to the shipping documentation from PackRight. Simms explained that he traveled several times a month and did not want to delay any business while he was away.

During Simms' trips, his administrative assistant used a stamped signature to approve shipping documents because they were expensive transactions that significantly impacted the business when delays occurred. Simms said he usually penned his signature for the packaging department paperwork, which was not as urgent and could wait until his return.

Mooreland was uncomfortable with Simms' delegation explanation. He understood the need to conduct business efficiently, but it didn't make sense to delegate that authority to an administrative assistant. Simms' direct report, Bill Michaels, the vice president of Logistics, would know more about the activities involved and could sign the documents while Simms was traveling.

Mooreland asked Simms about the strange delegation of authority. Simms replied that he didn't trust Michaels to sign for him. He explained that Michaels had tried to get involved before and Simms had to meet with human resources to make sure that was not something he was authorized to do.

The signatures varied depending on the type of document Simms was signing. Mooreland suspected someone was forging Simms' signature.

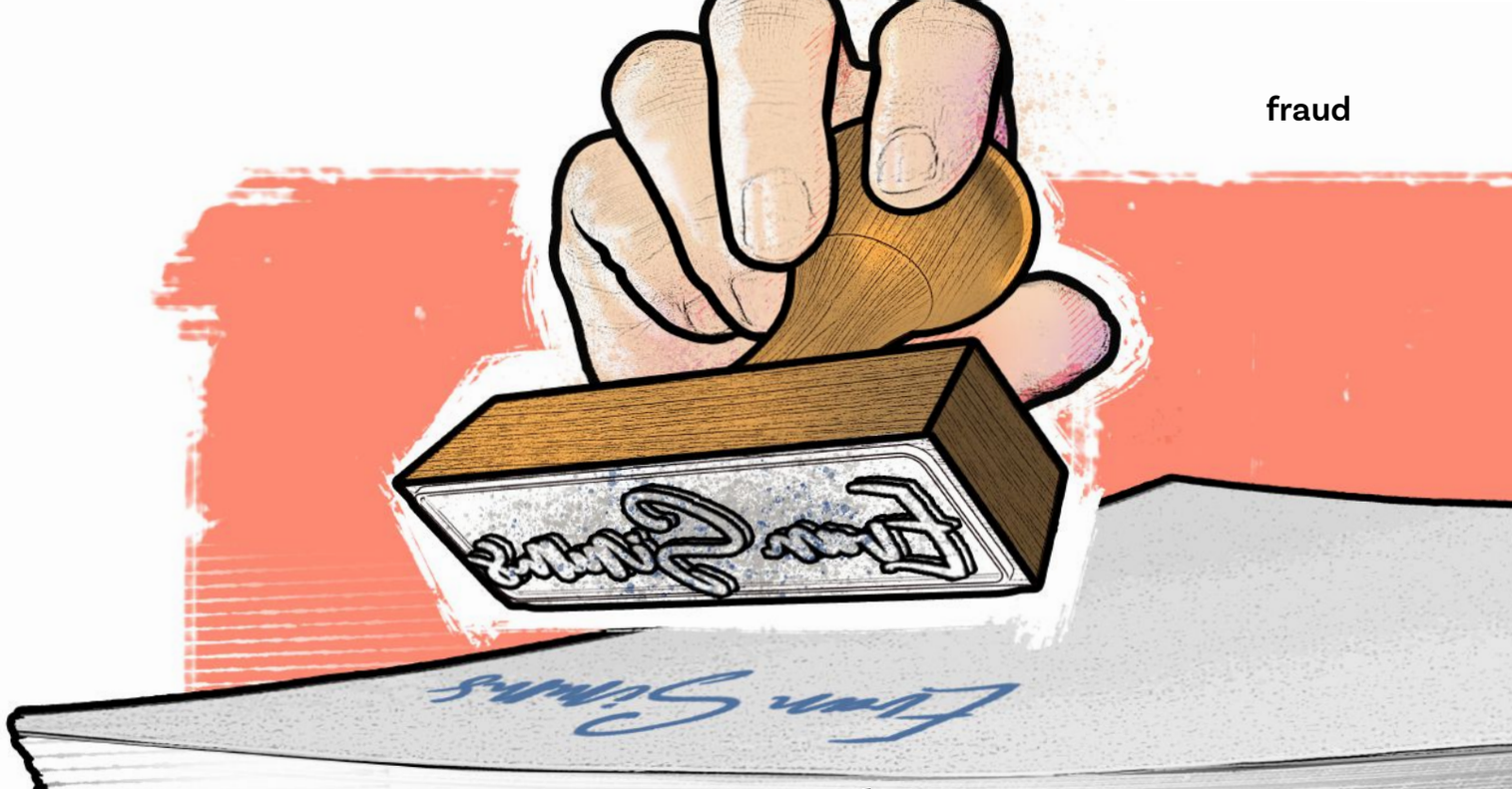
Simms answer shocked Mooreland, and the call left him with more questions. In fact, the conversation only complicated what he thought he had discovered. Instead of a simple but poorly executed forgery scheme, something much bigger could be happening.

He decided to look closer at the packaging activities and the outsourced shipping function. Mooreland studied the documents with the questionable signatures and noticed most of them were only PackRight documents, and not documents from other shipping vendors PoGo used.

Trusting his gut, Mooreland began looking deeper into PackRight's ownership and how it did business, and he was taken aback by what he found. Simms was listed as a co-owner of PackRight, which was created shortly after PoGo's decision to make its supply chain more efficient.

He had made sure no one would catch on by having

It was a clear violation of strict policies PoGo and MindSweep had in place to prevent conflicts of interest and undisclosed related-party activities.



his assistant approve these transactions instead of his direct report. Contracting with PackRight enabled Simms to funnel millions of dollars to his offshore company through inflated pricing mechanisms, which were often 15% above the normal market price. Moreover, it was a clear violation of strict policies PoGo and MindSweep had in place to prevent conflicts of interest and undisclosed related-party activities.

When Mooreland approached him about his findings, Simms indicated nothing was wrong with the business arrangement because PackRight performed the services for which it was contracted. MindSweep elected to terminate Simms but not to press charges, and Simms joined another company shortly after the incident.

David Kirtland, CIA, CRMA, CPA, CFE, is vice president of Audit for JERA Americas LLC in Houston.

Laura Harris, CFE, is a research specialist for the Association of Certified Fraud Examiners in Austin, Texas.

Lessons Learned

- **Signature stamps make paperwork easier, but they can increase the possibility of fraud.** Anyone could use the stamp, and the signatory may not be aware of how the stamp is being used. Moreover, the person who receives the stamped documentation may not know if it was authentically approved.
- **Little discrepancies can lead to bigger problems.** Auditors should investigate even the smallest details that do not make sense. There are no bad questions when discussing an organization's financial matters.
- **Tone at the top sets the ethical culture.** When employees see the person above them being dishonest, it tacitly encourages them to do the same. For example, when a stamp is misused, it reinforces any inappropriate action employees may consider.
- **Auditors must be prepared for anything and follow their instincts to the end.** If Mooreland had stopped his investigation when Simms mentioned both signature versions were authorized, he might not have found the undisclosed conflict of interest.
- **Related-party transactions should be disclosed for full transparency.** Inadequate disclosure of related-party transactions transcends all business types and relationships and is not limited to any specific industry.

new horizons.
NEW OPPORTUNITIES.

Join us in Washington, DC as internal audit experts, thought leaders, and practitioners from around the world provide cutting-edge insights and practices. It is an empowering experience to enhance skills, explore tech trends, and navigate evolving business risk landscapes globally.

MEMBERS CAN SAVE $570 on In-Person Registration • ***REGISTER TODAY*** • *theiia.org/IC*

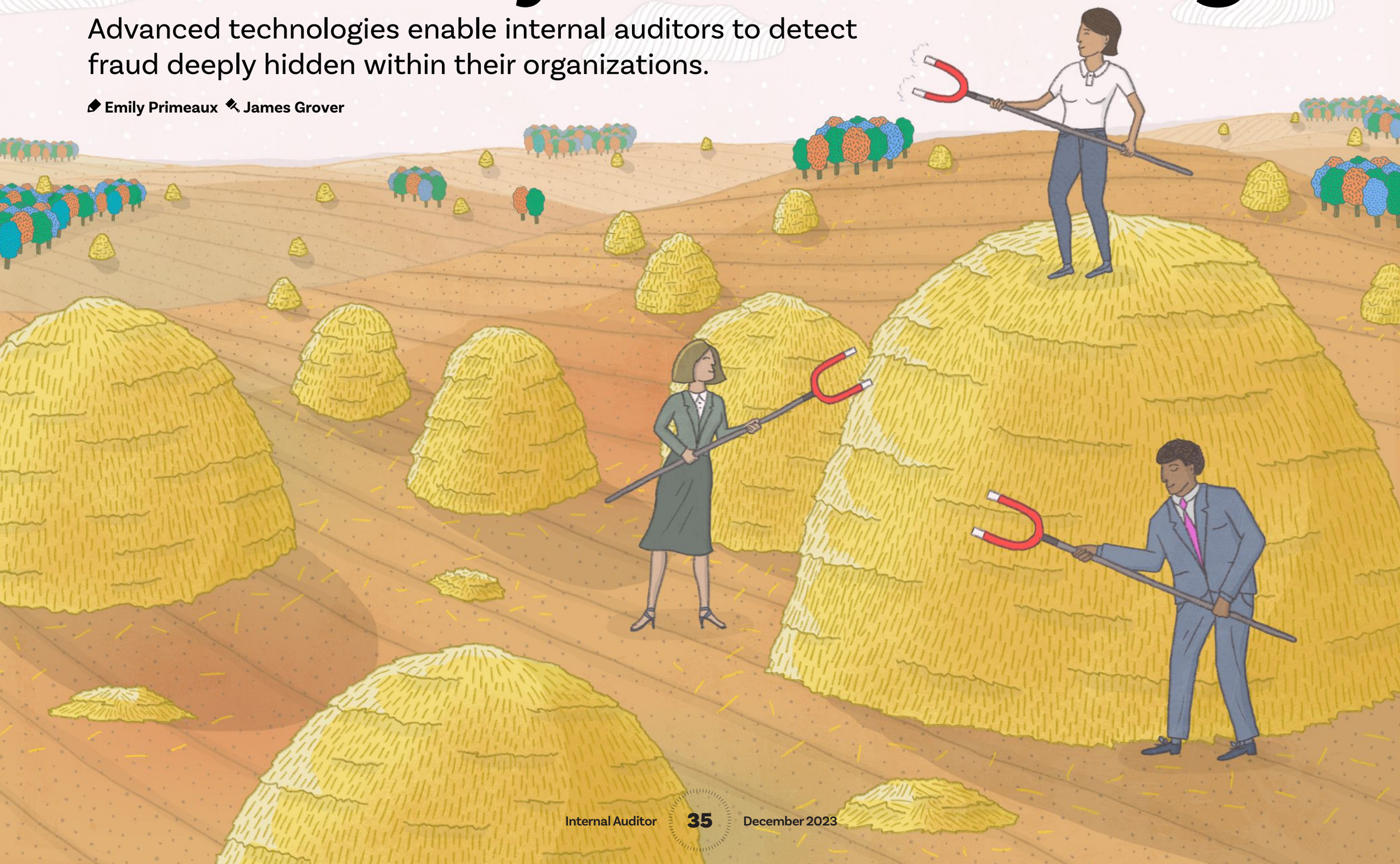
IIA INTERNATIONAL CONFERENCE
WASHINGTON, DC • 15-17 JULY 2024

2023-7208

The Analytics *Advantage*

Advanced technologies enable internal auditors to detect fraud deeply hidden within their organizations.

Emily Primeaux James Grover



Fraud risk is inevitable, no matter an organization's size or function. Acknowledging the risk is half the battle. Financial losses from fraud equate to 5% of company revenues, with half of cases attributed to internal control weaknesses, according to the Association of Certified Fraud Examiners' (ACFE's) 2022 Report to the Nations. Organizations that turn a blind eye to these risks are more likely to suffer long-term damage from a fraud event.

This is where data analytics can be a powerful ally for internal auditors. "Analytics has reshaped fraud detection and investigation in a significant and positive way," says Grant Ostler, industry principal at Ames, Iowa-based Workiva.

By efficiently processing large datasets and pinpointing irregularities, data analytics tools can highlight red flags of fraud that merit further examination by auditors. This collaborative approach between auditors and analytics enhances the audit process, bolstering an organization's safeguards against fraud and ensuring a more comprehensive and resilient strategy for managing fraud risk.

Where past internal audit analytics tools were made for users with IT or database skills, that has changed recently. "These tools have evolved and become more user-friendly, so analytics have been able to penetrate further into the world of audit," says Ken Petersen, director, product manager at Tampa, Fla.-based Wolters Kluwer TeamMate.

The availability of advanced analytics tools is just the tip of the iceberg, though. The real challenge lies in ensuring that internal auditors are adept at using these tools to their full potential, assessing the validity and integrity of the data being analyzed.

Quality Data Is Key

Even the most sophisticated analytics tools are only as reliable as the data fed into them. Petersen says a project's primary analytics challenge, be it for internal audit or otherwise, is securing access to the right data. Whether the project is an audit or an analysis of sales, help desk tickets, or voter demographics, users must start with good data, or the analysis will be wrong because the data was wrong or incomplete. Without high-quality data, even the most advanced analytics capabilities are not fully realized.

In addition to completeness, data quality is impacted by factors such as accuracy, validity, and timeliness. Tampering by individuals adept at deception also can weaken the quality and integrity of data, Petersen says.

Petersen underscores the importance of ensuring data integrity from its origin to its eventual use in a fraud case. He advocates entrusting the data to professionals well-trained in fraud investigations, such as fraud examiners or the legal team, given their familiarity with evidence trails (see "Fraud Fighters Unite" on page 39).

Vince Walden, CEO of KonaAI, a software provider based in New York, says with quality data, modern analytics tools are primed to cost-effectively elevate fraud detection and prevention efforts beyond traditional methods such as sampling. "Random sampling is good for testing business processes or a mathematical calculation, but horrible for effective fraud prevention and detection," he says. "It's like finding a needle in a haystack." He explains that fraudsters are proficient at hiding their crimes from old-school audit methods such as sampling.

"Random sampling is good for testing business processes or a mathematical calculation, but horrible for effective fraud prevention and detection. It's like finding a needle in a haystack."

—**Vince Walden**, CEO, KonaAI

"By analyzing data from multiple systems, auditors move from a two-dimensional view of transactions to a more three-dimensional, holistic view that can correlate transactions to underlying behaviors or processes."

—**Grant Ostler**, Industry Principal, Workiva

Instead, Walden advises using analytics tools to scrutinize and risk-rank all available data so that those transactions hitting multiple risk indicators rise to the top for review. For example, imagine risk scoring 250,000 invoices from highest to lowest risk and only needing to review the top 10 or 25. "How much better is that than hoping a random sample of 250,000 will turn up anything?" he asks.

Walden also emphasizes the indispensability of effective case management, if internal audit is to integrate machine learning into its continuous monitoring efforts, which can enable auditors to train the model by tagging high-risk transactions. "When I see a transaction, I can quickly tag it and create an alert for further review and validation," he explains, "which in turn teaches the model to be on the lookout for more like this."

From there, Walden says, analytics tools have a review pane where internal auditors must answer questions like, "How confident are you that this is an issue?" As an auditor tags answers there, they train the model. By answering analytics e-discovery questions, internal auditors give attributes to the transaction and build that predictive model.

"Analytics tools can uncover several unknown risks through full population testing that otherwise would not surface with sample-based testing," Ostler agrees. Testing entire populations provides more actionable and predictive analysis and recommendations. "By analyzing data from multiple systems, auditors move from a two-dimensional view of transactions to a more three-dimensional, holistic view that can correlate transactions to underlying behaviors or processes," he says.

Continuous Audits

To get a clearer picture of fraud risks, auditors should use data analytics tools to analyze unstructured data sources, says James Ruotolo, senior director, financial services at SAS, in Hartford, Conn. Beyond examining tables and structured data, this approach empowers auditors to transition from sample-based audits to comprehensive examinations of entire data populations. This includes content that previously might have been out of reach.

Automating this process can yield richer insights, facilitating easy correlation and cross-referencing. It also helps make continuous auditing and monitoring possible.

Ruotolo also encourages auditors to move toward continuous monitoring or continuous auditing. The increasing availability of vast data sets and the enhanced technology to analyze this data is making continuous monitoring a popular option. Unlike annual audits, this modern approach allows for automated and continuous oversight of specific business activities.

From a fraud detection standpoint, this evolution is particularly promising. Analytics and data management tools help auditors organize, clean, and analyze large troves of data so that they can truly take advantage of that data. By implementing basic analytic capabilities, setting up dashboards, and establishing business rules, auditors gain a clearer direction for their audit work. Analytic insights can guide auditors on what areas might require more intensive scrutiny during on-site audits.

In more advanced scenarios, continuous monitoring can even detect suspicious activities in real time, Ruotolo says. When these

"At some point, [internal auditors] have to go deeper, past the analytics, which is an important conversation now as AI is being spotlighted."

—**Ken Petersen**, Director, Product Manager, Wolters Kluwer TeamMate

irregularities are spotted, auditors can immediately address them. This might involve alerting a specialized investigative team or, in some cases, the audit team, itself, can intervene directly to resolve the identified issue.

Balancing Analytics With Auditor Expertise

Even as these capabilities bring new possibilities, internal auditors must remain vigilant while harnessing the power of advanced analytics tools. Petersen recalls an internal audit case where analytics flagged higher costs for cleaning supplies at a mass transit system compared to previous years. Upon discovering the discrepancy, auditors used analytics to determine what the differences were in items purchased between the two years.

Their analysis found increases in items that didn't make sense for cleaning a mass transit system, such as large purchases of microfiber cloths. Moreover, they determined that the supplies weren't being used or stored in inventory. Using tools designed to track phone calls, auditors found unusual communication activity between the employee purchasing the items and a person working for the vendor.

The investigation discovered that the employee was purchasing supplies and selling them at a profit for his own gain. In this case, analytics helped detect anomalies, but it was internal auditors who found the fraud.

"At some point, we have to go deeper, past the analytics, which is an important conversation now as AI is being spotlighted," Petersen says. "Internal auditors have a unique skillset — sifting through information, deciphering it, and going back to the paper trail to find the deception."

Walden highlights the importance of the internal auditor's involvement when setting up analytics tools. Without the auditor's knowledge, the analytics tools won't know what to test. "When you risk score, you come up with your segregation of duties tests, conflict of interests tests, and fraud controls — you thoughtfully create 15 to 100 tests," he explains. "Then you pour 100% of your data through those tests. Doing this creates an objective, repeatable process for selecting better audit samples."

Effective fraud tests should consider a few principles. It's crucial to continually update and adapt fraud tests to address evolving risks and changing business processes. Tests also should consider financial data and nonfinancial indicators, such as employee behavior and communication patterns, that can offer valuable insights into potential fraud. Departments such as finance, legal, and IT should collaborate to ensure tests are comprehensive and well-rounded, and test results should be thoroughly analyzed and remediated quickly to mitigate additional risks and strengthen internal controls.

Start Small, Then Expand

Although fraud analytics tools can require a sizeable investment, their ability to detect transactions in real-time can prevent sizable financial losses. ACFE estimates that a typical fraud takes 12 months to detect, with $8,300 in monthly losses. Internal auditors may feel trepidatious as analytics become more technologically complex and involved.

Ruotolo recommends the "crawl, walk, run" strategy for getting started. "The best approach is to start small," he says. "Pick a project that's basic, starts producing value, and is giving results. Then you can expand from there."

Key lessons from the first project include who "owns" the data and what approvals are required to use it, where there are data gaps, and

whether the organization has the right tools, resources, and training to successfully implement a data analytics project. Once auditors demonstrate success, Ruotolo recommends rolling the approach out to other parts of the organization. From there, the organization can enhance the tool or deploy more advanced types of analytics or capabilities.

Getting buy-in from management also may come easier by starting small and expanding later. Ruotolo says he sees companies insist that they need enterprisewide internal audit analytics for all use cases, and they will spend two years trying to build analytics, models, and rules. After 18 months, executives start to ask why they have spent so much money but haven't seen results. "Starting small will bring quick wins," he says.

That is why it is essential for internal audit to establish a clear scope of reporting to the audit committee and senior leadership about the ongoing progress of the fraud analytics project, Ruotolo says. Regular reporting not only keeps them in the loop but also provides them with key performance indicators (KPIs), milestones, and progress updates. KPIs could include false positive rates, detection rates, time to detection,

It is essential for internal audit to establish a clear scope of reporting to the audit committee and senior leadership about the ongoing progress of the fraud analytics project.

—**James Ruotolo,** Senior Director, Financial Services, SAS

Fraud Fighters Unite

While the debate over the precise role of internal audit in fraud detection continues, beneath the surface of these discussions lies a shared commitment: Internal auditors are united with fellow anti-fraud professionals to safeguard their organizations. They often share insights, methodologies, and perspectives on fraud investigation and auditing. This overlapping interest is more than just coincidental — it signifies a deep-rooted alignment in purpose and approach.

Last year's announcement of a partnership between the ACFE and The IIA aims to spearhead educational initiatives that cater to the intertwined interests of both memberships. By pooling resources and expertise, the partnership promises to elevate the standards of fraud investigation and auditing.

"The purpose of the partnership is so we can work with The IIA to give their members and internal auditors more tools and information to help them in their fraud prevention and detection efforts," says John Gill, president of the ACFE. "I'm always impressed with the internal auditors I have met in our classes. They are committed to adding more tools to their toolbox."

John Gill, president, ACFE

investigation time, and average loss per fraudulent transaction.

Ruotolo says the "crawl, walk, run" strategy is particularly effective in this context. This incremental approach often garners positive feedback from senior executives, who are more likely to fund future endeavors when they witness tangible value emerging from their investments.

Effective communication is more than just about frequency, though. For instance, ACFE's anti-fraud playbook emphasizes the importance of the fifth pillar of COSO's *Enterprise Risk Management–Integrating With Strategy and Performance* framework, which highlights program monitoring. One of its key recommendations is ensuring that the insights shared with front-line operations should differ from those presented to senior executives.

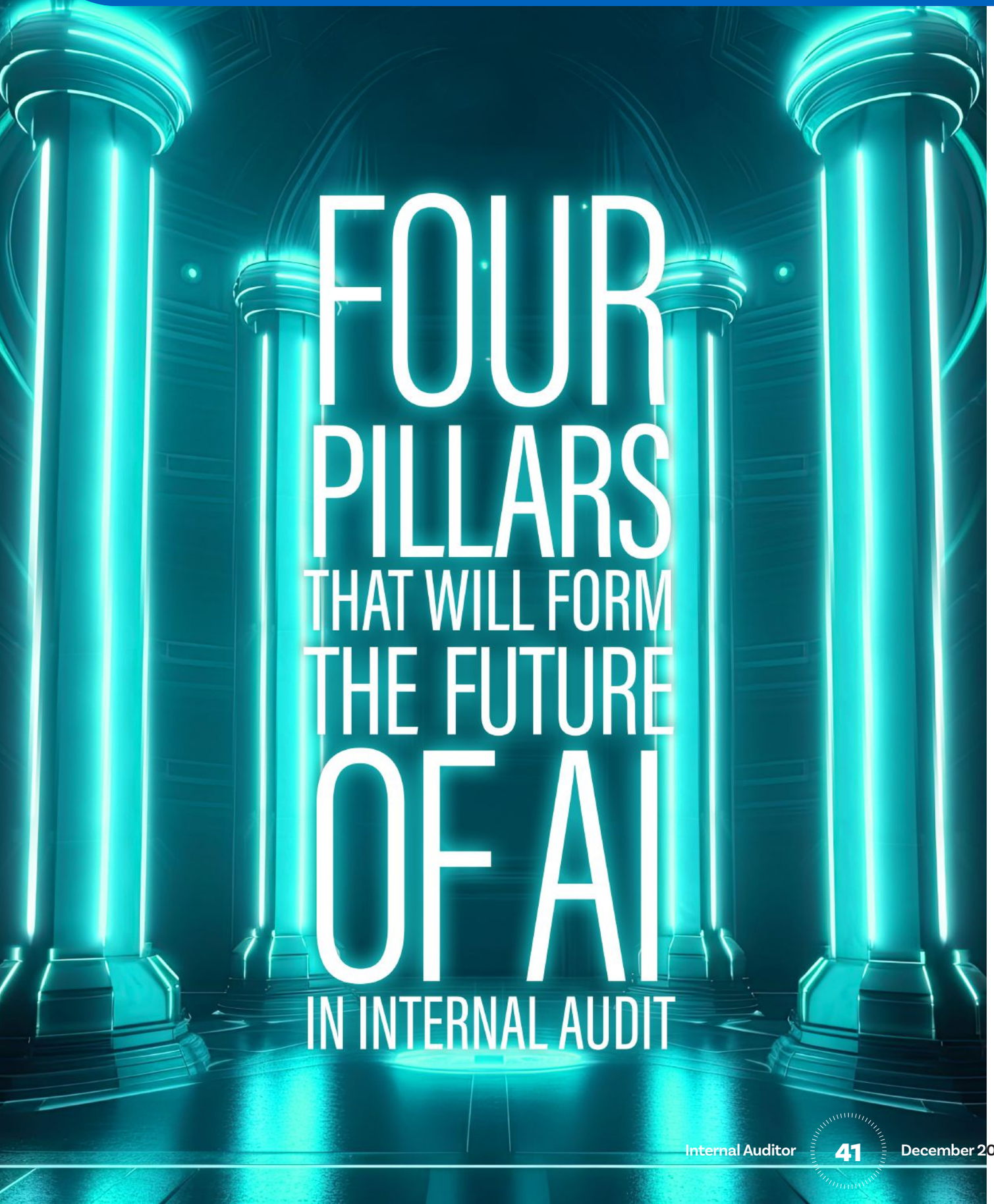
Internal audit should be clear about its objectives when communicating with senior leadership. Whether seeking approval, additional funding, or more personnel, auditors should present all the necessary information to help executives make well-informed decisions. "The impact internal audit can have on reducing the risk profile of their organization is compounded by sharing those analytics with management," Ostler says.

The convergence of advanced data analytics and internal auditing is reshaping the way organizations approach fraud, making the audit process more dynamic, precise, and proactive.

Reshaping Fraud Fighting

As data becomes increasingly integral to fraud detection, internal auditors equipped with advanced analytics capabilities are better positioned to identify and address potential risks. The convergence of advanced data analytics and internal auditing is reshaping the way organizations approach fraud, making the audit process more dynamic, precise, and proactive. In this data-driven era, the collaboration between analytics and internal auditing is not just beneficial — it's essential for organizational resilience.

Emily Primeaux, writing manager at Dragonfly Editorial and former associate editor at *Fraud Magazine*, is based in South Florida.



FOUR PILLARS THAT WILL FORM THE FUTURE OF AI IN INTERNAL AUDIT

Internal auditors are looking for ways to adopt new digital solutions without losing the integrity of data privacy for the organizations they support.

By Pam Hrubey and Amanda Marderosian

For internal audit, AI presents the opportunity to increase efficiency in data analysis, risk assessment, automated testing, fraud detection, documentation and reporting, continuous monitoring, and more. If applied appropriately, it can save time by tackling field work and initial processing so auditors can focus elsewhere.

While beneficial, the introduction of AI in internal audit can pose security challenges for internal auditors and their employers. Auditors may find themselves asking questions like: Are the correct controls in place? Is access to relevant data approved? Has the team reviewed relevant data processing policies? Do data processing policies include guidance for use of AI?

Internal auditors must be leaders in data application, analysis, and safety. Mindful of the desire to lead, how can internal audit use AI safely to make the function more successful? How can the use of AI deliver more valuable results without the risk of human error or inadvertent data leaks?

With the rise of AI, internal auditors must develop processes that maintain transparency, promote good governance, and facilitate operations with ethics, efficiency, and compliance, all while safeguarding their most precious commodity: data.

To address these concerns, Crowe suggests leveraging four pillars that will form the future of internal audit. This transformative approach aims to help internal auditors apply technologies with confidence, strategize with new insights, and perform with assurance.

PILLAR 1

Be Human

Audits provide information, but it is up to humans to turn this information into something of value. Strategic communication and goal setting can help humans drive desired value. Instead of seeing the audit as just a task, internal auditors can look at who their audits will help and how to best address their goals. Embracing new technologies like AI can help auditors achieve their goals by providing more time for them to focus on being human and building relationships with team members, while AI handles more of the repetitive tasks. To promote data privacy, internal auditors can learn from their internal privacy teams to gain insights for their audits and develop a plan that will help all parties succeed and maintain safe data practices and data integrity.

PILLAR 2

Get More Strategic

The addition of AI can free up more time for internal auditors to think strategically about their findings and future recommendations. Auditors can leverage AI algorithms to quickly capture and monitor historical data, identify problem areas, and predict potential future risks that inform next steps. Audit teams can use natural language processing to analyze regulatory updates simplifying the maintenance of compliance requirements. AI can also be used to develop benchmarks for the organization compared to industry standards. Leveraging benchmarks can help internal auditors provide more value to stakeholders, which can help inform future strategic decision-making.

PILLAR 3

Gather (And Use) Smarter Data

AI can provide internal auditors with quicker access to smarter data at scale. The more data used at scale, the better the analysis. AI can be used to automate data extraction, saving time and reducing the potential for human error. Using AI in predictive analytics models can expedite forecasting potential risks and trends. Through continuous monitoring, AI helps internal auditors identify patterns, enhance fraud detection, and monitor financial transactions. Through pattern recognition, AI can help auditors identify intricate patterns in large data pools quickly, which helps audit teams deliver value more quickly.

PILLAR 4

Leverage Technology

Historically, many internal audit processes have been manual. AI presents the opportunity to automate time-consuming manual tasks, freeing up time for auditors to focus on more pressing concerns, like risk management, fraud detection, and governance and compliance. AI-related technology supports numerous process enhancements like continuous monitoring. Be sure to factor in privacy safeguards like data anonymization and data localization to limit third-party interactions, consider building training modules to educate auditors and staff, and more.

The Future of Internal Audit

AI presents opportunities for internal auditors to become more effective strategic business advocates for the organizations they support. While it is the auditors that make internal audits so valuable to organizations, technology like AI can help give auditors time back in their days, automate painstaking manual tasks, and streamline and simplify processes, creating the opportunity for auditors to operate more strategically and deliver greater value.

Download the "internal auditor's AI safety checklist" at www.crowe.com/iia.

Pam Hrubey is chief privacy officer at Crowe.

Amanda Marderosian is privacy, data protection, and compliance manager at Crowe.

> CERTIFICATION

Certified *for Success.*

Success is measured by the impact you make.

Make an impact by earning the Certified Internal Auditor® (CIA®) credential. CIA will distinguish you from your peers and prove credibility and proficiency. Wherever your journey takes you, CIA will certify success.

Improve credibility. Prove proficiency. *www.theiia.org/CIA*

CIA® Certified Internal Auditor®

FOCUS ON RISK

The Internal Audit Foundation and the broader IIA combine forces to survey the global risk landscape.

Neil Hodge

nternal audit leaders report cybersecurity, human capital, and business continuity will be the three highest risks for their organizations globally in 2024, according to Risk in Focus Global. They say these risks will continue to feature prominently three years from now but also expect climate change and digital disruption risk to grow rapidly and become key areas of focus.

Risk in Focus Global is a collaboration guided by the Internal Audit Foundation with support from IIA regional bodies, IIA affiliates, and corporate sponsors. The Risk in Focus concept was created in 2016 by the European Institutes Research Group, which continues to publish the reports through the European Confederation of Institutes of Internal Auditing. The project was conducted worldwide for the first time in 2023.

Javier Faleato, executive vice president of Global Strategy & Affiliate Relations at The IIA and executive director of the Internal Audit Foundation, has been involved with publishing the reports since 2016. He says he has watched the reports "evolve to become an indispensable tool for CAEs in developing their annual internal audit plans."

Reporting on the Risks

In addition to a Global Summary of Survey Results, Risk in Focus includes a Hot Topics report for internal auditors and a Board Briefing for stakeholders for each of The IIA's six regions — Africa, Asia Pacific, Europe, Latin America, Middle East, and North America. The reports highlight not only the key risks for organizations and the core areas of focus for audit functions in each region, but also the drivers behind why the risks are rated so highly.

Cybersecurity. Interestingly, the reports show that not all regions perceive risks in the same way. For example, in North America, cybersecurity risk is fueled

The reports highlight not only the key risks for organizations and the core areas of focus for audit functions in each region, but also the drivers behind why the risks are rated so highly.

Risks Worldwide

not only by the rise in malicious attacks such as ransomware and malware, but also by the influx of regulatory reporting requirements around cybersecurity and breach reporting. However, for CAEs in Africa, cybersecurity is a primary concern because as countries' IT infrastructures become more technologically advanced, so too do the levels of attack on their systems.

Nor do CAEs in different regions apportion the same amount of audit effort to these risks. For example, there is a wide gap in terms of the effort spent on cybersecurity: In North America, 84% of CAEs say cybersecurity is one of their five key focus areas, compared to a global average of 68%.

In North America, cybersecurity dominates the internal audit agenda, and it will likely remain the primary risk into 2027 — fueled in part by a new requirement adopted in July by the U.S. Securities and Exchange Commission for reporting incidents and disclosing activities related to cybersecurity risk management, strategy, and governance. These rules are layered on top of a raft of existing cyber regulations, thereby accounting for much of internal audit's focus.

Human Capital. Meanwhile, human capital remains the second biggest risk organizations face worldwide, according to the survey. Fifty-one percent of CAEs identify it as a top five risk. They say they expect it to remain in the top five through 2027.

And it's not just an organizational problem — internal audit functions also are finding it hard to hire and keep staff. Several have restructured their talent pipelines to promote diversity among candidates who are making their way up the promotion ladder. But staff retention is a problem.

"Out of a team of 20, in the last 18 months I've lost 10," says one CAE in Europe. "As we attract a more diverse range of people from the business, we find they have more choice about where to go as a next step."

In addition, attracting younger workers to form talent pipelines is not as

In North America, cybersecurity risk is fueled not only by the rise in malicious attacks such as ransomware and malware, but also by the influx of regulatory reporting requirements.

North America

Asia Pacific

easy as it once was. Many increasingly challenge the core values that underpin the corporate focus and demand clearer action from companies to address issues such as their environmental impact and the steps they take to improve opportunities for female, minority, and LGBTQ+ employees. Younger workers also are more likely to be vocal in their desire to back hybrid, remote, and flexible work.

In the Asia Pacific region, human capital is a top risk for very different reasons: Geopolitical and macroeconomic uncertainty in neighboring countries have impacted organizations' ability to attract and retain the right talent and skills. For example, during the pandemic, many skilled foreign workers left Singapore, returned to their home countries, and did not come back after the pandemic eased, leaving critical roles unfilled.

Audit effort for human capital is relatively low compared to risk: 51% of CAEs worldwide see human capital as one of their top five risks, but only 30% say it is one of their top five areas for audit time and effort.

Business Continuity. Another major concern worldwide is business continuity, but in this case, audit focus (54%) is more closely matched with organizations' perceived level of threat (47%).

Concerns about business continuity were highest in Asia Pacific (61%) and the Middle East (53%), with CAEs citing lessons learned from the worldwide impacts of COVID-19. "Since the pandemic, we have been changing the mindset within the business so that management thinks about what could go wrong as a kind of general practice in all decisions," says a CAE from Saudi Arabia.

To ensure business continuity plans work, CAEs say they look for the hidden links between seemingly independent risk categories. To proactively prepare for disruptions, internal auditors are rethinking business models and supply chains. CAEs say it is important to use leading indicators rather than rely

In the Asia Pacific region, geopolitical and macroeconomic uncertainty in neighboring countries have impacted organizations' ability to attract and retain the right talent.

on lagging indicators to ensure business continuity plans remain robust, flexible, and agile.

"Our biggest emerging risk is the ability of every part of the organization to critically identify what-can-go-wrong scenarios even before risks hit," a CAE at a Philippines-based electronics company says.

Fraud. As the reports show, some regions face their own unique challenges. Africa, for example, stands out for having fraud among its top five risks: In fact, fraud risk currently ranks highest for internal audit time and effort in Africa. Fifty-seven percent say it is a top five area, compared to just 26% of respondents in North America. However, three years from now, fraud risk is expected to become less time consuming and drop to fourth as digital disruption and climate change rise on the agenda and become second and sixth highest, respectively.

CAEs say fraud risk is prominent in Africa because incidents of bribery and corruption historically have been high. At the same time, the methods used by internal audit functions to detect and combat fraud are becoming more technically sophisticated.

Ruth Doreen Mutebe, CAE at Ugandan power company Umeme and chair of the African Federation of Institutes of Internal Auditors, says internal auditors are learning to use enterprisewide data analytics to identify fraud by automatically identifying exceptions in a wide range of areas — from procurement to human resources. Auditors can then quickly follow up on unusual activity and act before it turns into a major issue. "Internal auditors need to enhance their skills in data analytics and allocate budgets to systems that support it," Mutebe says.

Geopolitics. Geopolitical risks can churn for years or flare up dramatically — as the violent conflict between Israel and Hamas demonstrates. At the time of the Risk in Focus survey (February to July 2023), geopolitical risks were highest in Latin America and Europe.

Africa stands out for having fraud among its top five risks: In fact, fraud risk currently ranks highest for internal audit time and effort in Africa.

Africa

Political disruption in Latin America is exacerbated presently by the fact that between 2021 and 2024, every country in the region is set to face at least one major election. Such quick turnarounds in political power can result in sweeping legislative and regulatory changes, as well as appetites for enforcement.

As a result, CAEs in the region say internal auditors need to proactively monitor emerging risks and their impacts on customers and supply chains and assess how they interact. "Politics, the environment, trade barriers, macroeconomic risks — you need to combine these threats and have a holistic view so that you can advise management how they should act," says Fábio Pimpão, director of internal audit at Whirlpool Latin America.

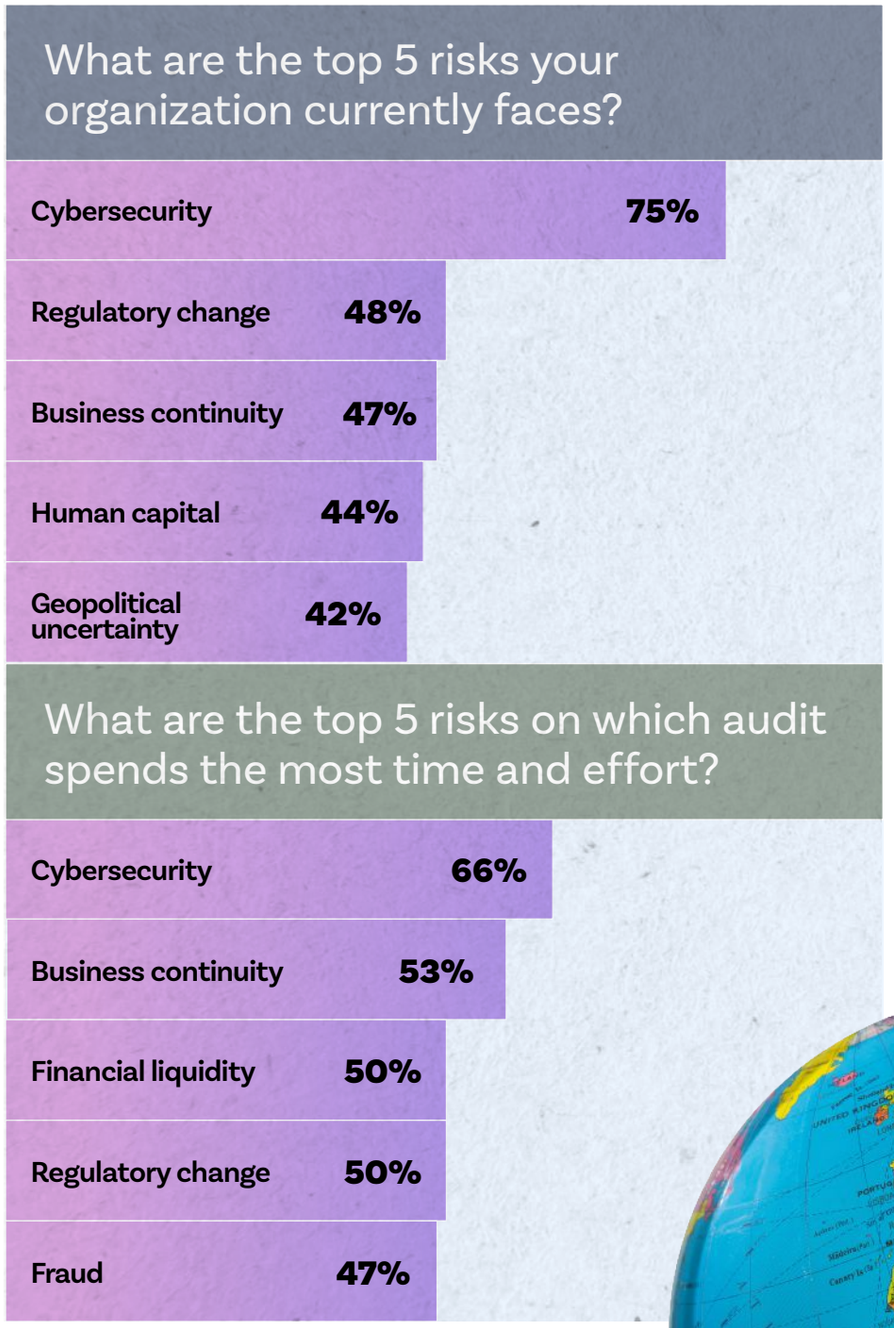
In particular, CAEs should create scenarios to ensure the business maintains enough financial liquidity during a crisis. "In the end, what is going to break a company is not the P&L account … or reporting failures — it is going to be cash flow," Pimpão explains. "Scenarios of emerging risk can help determine when internal audit needs to focus on cash management, for instance, to give some strategic recommendations that aid corporate decision making to avert disaster."

Europe ranked geopolitical uncertainty as its third highest area of concern, as organizations deal with Russia's invasion of Ukraine and western governments' unsteady relations with China. Also, the macroeconomic impacts — rising inflation, higher interest rates, the cost-of-living crisis — are a particular challenge in the region, as many European companies do not have the budgets to spend on strategic development programs that competitors in other parts of the globe might have at their disposal (especially in lower-cost countries such as China).

"You are beginning to see an environment where it is not that easy for companies to strategically invest in R&D and innovation for

Political disruption in Latin America is exacerbated presently by the fact that between 2021 and 2024, every country in the region is set to face at least one major election.

Latin America



the future," a professor of internal auditing and corporate governance in Germany responds. "This will be a major risk for European businesses because competitors in the U.S. and China do not face the same complexity of macroeconomic and political risk."

Closing the Gaps

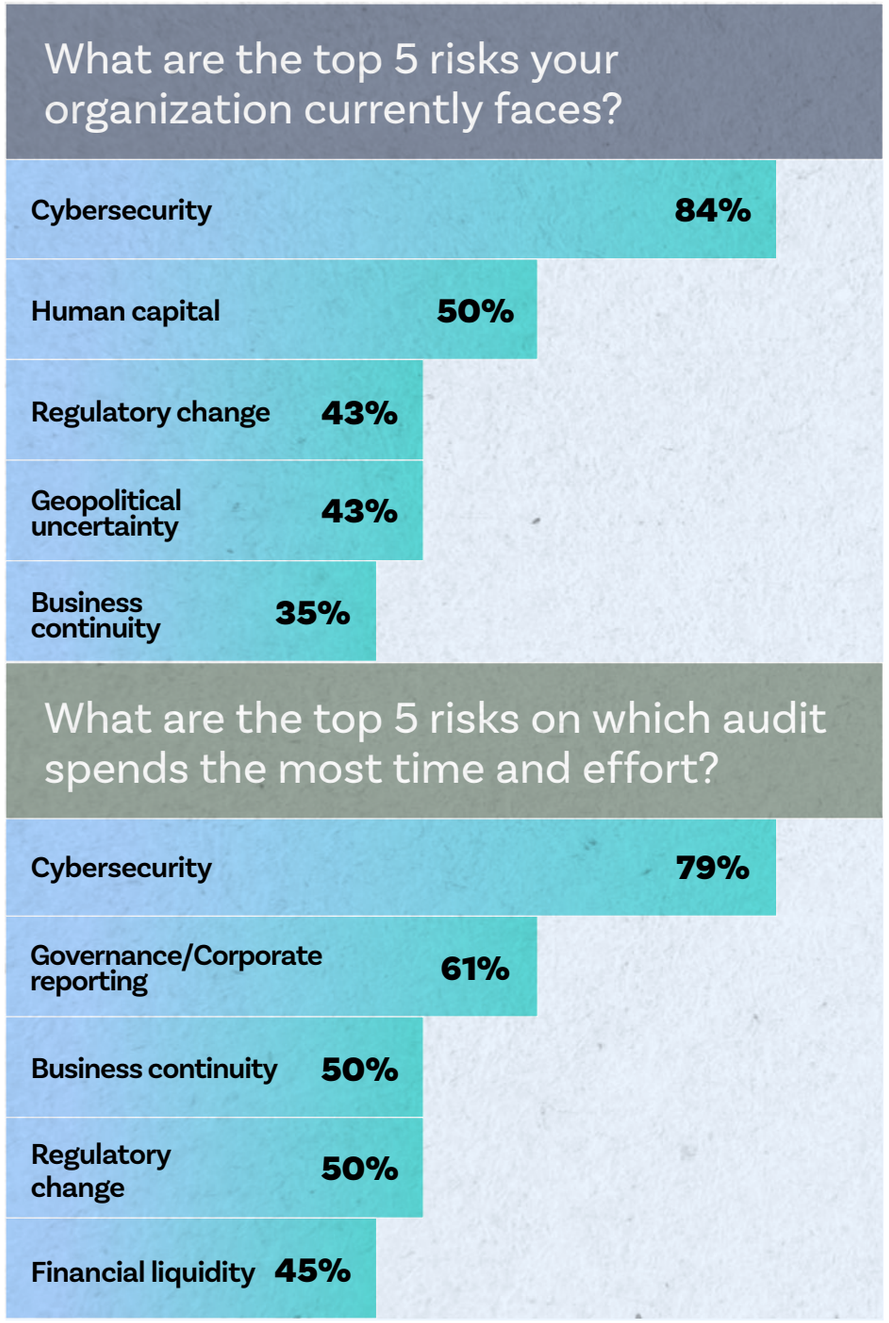
Faleato says one of the key highlights of the reports is that they show in each region of the world the level of alignment — or misalignment — between what organizations believe are the key risks to their business and where internal audit effort is focused. "Alignment is getting better," he says.

"Where there are still gaps between the level of perceived risk and the amount of internal audit effort, it usually comes down to a lack of knowledge and skills," Faleato says. "For example, climate change still ranks relatively low in terms of internal audit focus because some organizations are still immature when evaluating or reporting the environmental impact of their operations. Similarly, digital disruption is a new and evolving risk and requires more specialist knowledge to understand, and audit functions have recognized they need to do more."

Faleato says he hopes the reports become a valuable resource that enables internal auditors to begin a conversation with the board and top management about which risks are important for their organizations in different regions. "I want them to open up a conversation about whether the level of audit focus is matched to the risks the board has prioritized, and what action boards should take if there are gaps," he adds.

Neil Hodge is a freelance journalist based in Nottingham, U.K.

Europe



Europe ranked geopolitical uncertainty as its third highest area of concern, as organizations deal with Russia's invasion of Ukraine and western governments' unsteady relations with China.

Master the Art of **Internal Audit!**

Choose from Six Virtual Conferences.

No need to travel. Attend any of these conferences from the comfort of your home or office, making it easier than ever to access vital audit knowledge and earn CPE.

Fraud Virtual Conference • February 29

Analytics, Automation, and AI Virtual Conference • April 18

Sustainability Audit Risk Assurance Virtual Conference (SARA) • June 20

Enterprise Risk Management Virtual Conference • September 12

Cybersecurity Virtual Conference • October 30

AuditSphere: A Virtual Conference for Small Audit Teams • December 5

Learn more at theiia.org/VirtualConferences
now to reserve your place at all six conferences.
Don't miss these opportunities to excel in internal audit.

The Institute of
Internal Auditors

The Knowledge Audit

By categorizing and assessing two types of knowledge, internal auditors can help organizations manage intellectual capital.

David J. O'Regan Donough O'Malley

An employee leaves an organization, taking with her a storage device with documents she always kept "offline," outside of the organization's shared, networked repositories. A sincere but overenthusiastic marketing employee posts a social media message that alienates a large portion of a company's customers, triggering a consumer boycott. Sales drop at an online business because a customer service department lacks the necessary product details to satisfactorily address telephone queries — a sure way to accumulate poor online reviews. A CEO publicly eats humble pie, apologizing for a data security breach in which millions of customers' bank details were hacked.

The Knowledge Audit

What do these situations have in common? They are all failures of knowledge management, involving not merely the mishandling and inadequate protection of information but also its misuse, misapplication, and miscommunication.

Institutional knowledge management is a notoriously tricky topic for internal auditors to assess. However, by becoming familiar with some of the challenges involved in auditing knowledge, as well as some solutions, internal auditors can better protect the organization's intellectual capital.

Information & Expertise

When approaching any audit endeavor, an essential starting point is a definition of terms. This principle is especially important for knowledge management, given the potential ambiguities of the term "knowledge" and the multiplicity of concepts it encompasses. For audit purposes, there are two broad types of knowledge organizations should manage: information and expertise.

Information refers to facts and data, and it is likely the type of knowledge with which auditors have the most comfort. Expertise refers to how to interpret, act on, and

communicate information. Expertise is more challenging for both organizations and auditors, as it can sometimes be elusive to identify and tricky to protect.

Together, these two types of knowledge address how organizations identify, arrange, understand, use, protect, and transmit information. There are risk and governance issues specific to each, as well as challenges that cut across both categories.

Information Management

The information aspect of knowledge management is the most straightforward to audit. As a starting point, auditors typically assess how organizations identify their information, which may be scattered over a wide range of repositories. The concept of information should be construed as broadly as possible. Examples include accounting transactions, research and development records, the names and details of personnel, minutes of management meetings, market analyses, legal documentation, and the contents of an organization's social media accounts.

Some organizations differentiate between data and information, with data referring to raw facts and information referring to data that is organized and deployed for use. While the distinction is not universally used, it can be a useful way of coming to grips with this area.

Beyond identifying the information they possess, organizations should have a comprehensive security plan to safeguard the information from various threats. Information protection risks include the loss, theft, or corruption of information, including intellectual property as a formal, intangible asset.

Breaches of privacy and adherence to international privacy laws also are common concerns. Risks of this nature require robust preventive internal controls like reliable cybersecurity defenses, rigorous document management systems, and comprehensive recovery arrangements in case of the loss or corruption of information arising from lapses in security. Fortunately, these topics are well documented.

There are two commonly encountered informational risk considerations that auditors should bear in mind. First, the risk of information loss or incompleteness is heightened when employees store information outside an organization's approved channels.

Some individuals deliberately keep information in the shadows, refusing to share it and enjoying exclusive control over discrete pieces of knowledge.

This hazard arises in instances of a common behavioral trait: Some individuals deliberately keep information in the shadows, refusing to share it and enjoying exclusive control over discrete pieces of knowledge. By manipulating valuable information in this way, these individuals may create an impression of their indispensability to the organization. And the information they tuck away in some hidden electronic repository — or even a manually written notebook — is highly vulnerable to loss.

Organizations may introduce incentives to dissuade such dysfunctional behavior. In the case of departing personnel, an organization could require a supervisor to confirm that information has been successfully handed over before releasing separation payments to the exiting employee.

A second significant risk concerns information legitimately stored outside of an organization's official channels. For example, information is sometimes held jointly by two organizations, in arrangements like joint ventures and outsourced activities. Information may be even more widely diffused, in examples like a consortium of several organizations or along the length of a supply chain. This extramural information tends to be exceedingly difficult to capture and inherently risky to control, as it involves the sharing with outsiders of overlapping legal and moral responsibilities for its custody.

Internal controls over scattered information typically are established through cooperation among the organizations concerned. However, there might be gaps in the information held by one of the organizations involved, and there also might be legal and practical barriers to auditing shared information.

Expertise Management

The safeguarding of information involves considerations at the "hard" end of the knowledge spectrum. With expertise, internal auditors turn to the "softer" aspects of knowledge management. It is good that an organization possesses rigorously arranged and reliably protected information, but unless its workforce is capable of adequately understanding the information and applying and communicating it for practical purposes, the entire system of knowledge will be of limited value.

To optimize expertise as a branch of its knowledge, organizations should ensure that suitable hiring practices are in place to identify employees with the aptitudes and abilities to interpret and use information. Beyond the recruitment cycle, ongoing training and education encourage the maintenance and development of the necessary expertise.

The transmission of expertise from departing to remaining and future personnel is more challenging than the transmission of raw information. Expertise often is tacit and individualized in nature, yet it can

be captured and transferred, to a degree, through up-to-date training materials and comprehensive handover notes from departing personnel.

Internal controls over expertise are important to mitigate the risks of incorrectly interpreting and applying information. Misunderstandings of decision-making inputs and the mishandling of decision-making processes are typical outcomes of poorly managed institutional expertise. One example is an investment decision that relies on future, incremental cash flows: If staff are unaware of concepts like "sunk costs" they may include in their calculations costs that are irrelevant to the decision-making process.

Strategy & Culture

Identifying the two broad types of knowledge helps internal auditors conceptualize the risks and concerns applicable to the safeguarding and best use of information and expertise. In addition, there are risks that cut across both categories of knowledge management.

One concern is the organization's knowledge management strategy. The auditor's initial questions should be: Does such a strategy exist? If not, why not? And, if it does exist, does it comprehensively cover both categories of knowledge?

Further, is the strategy congruent with organizational objectives, and does it offer a practical roadmap for how to go about capturing, storing, sharing, using, and communicating information? A clearly defined strategy is needed to guide the allocation of resources and responsibilities for knowledge management.

Beyond strategy, auditors should evaluate an organization's culture of knowledge-sharing. A healthy culture of knowledge management overcomes institutional "silos" and establishes networks of cooperation and collaboration throughout the organization. Assessing the effectiveness of a knowledge management culture may cover:

- The organization's tone at the top in encouraging the sharing of information and expertise.
- The extent and nature of relevant training.
- The infrastructure available for sharing knowledge, including intranet sites, discussion boards, face-to-face interactions, and other communication tools that "socialize" topics of interest.

Internal audit also should evaluate any organizational methods for disseminating the lessons learned from audits.

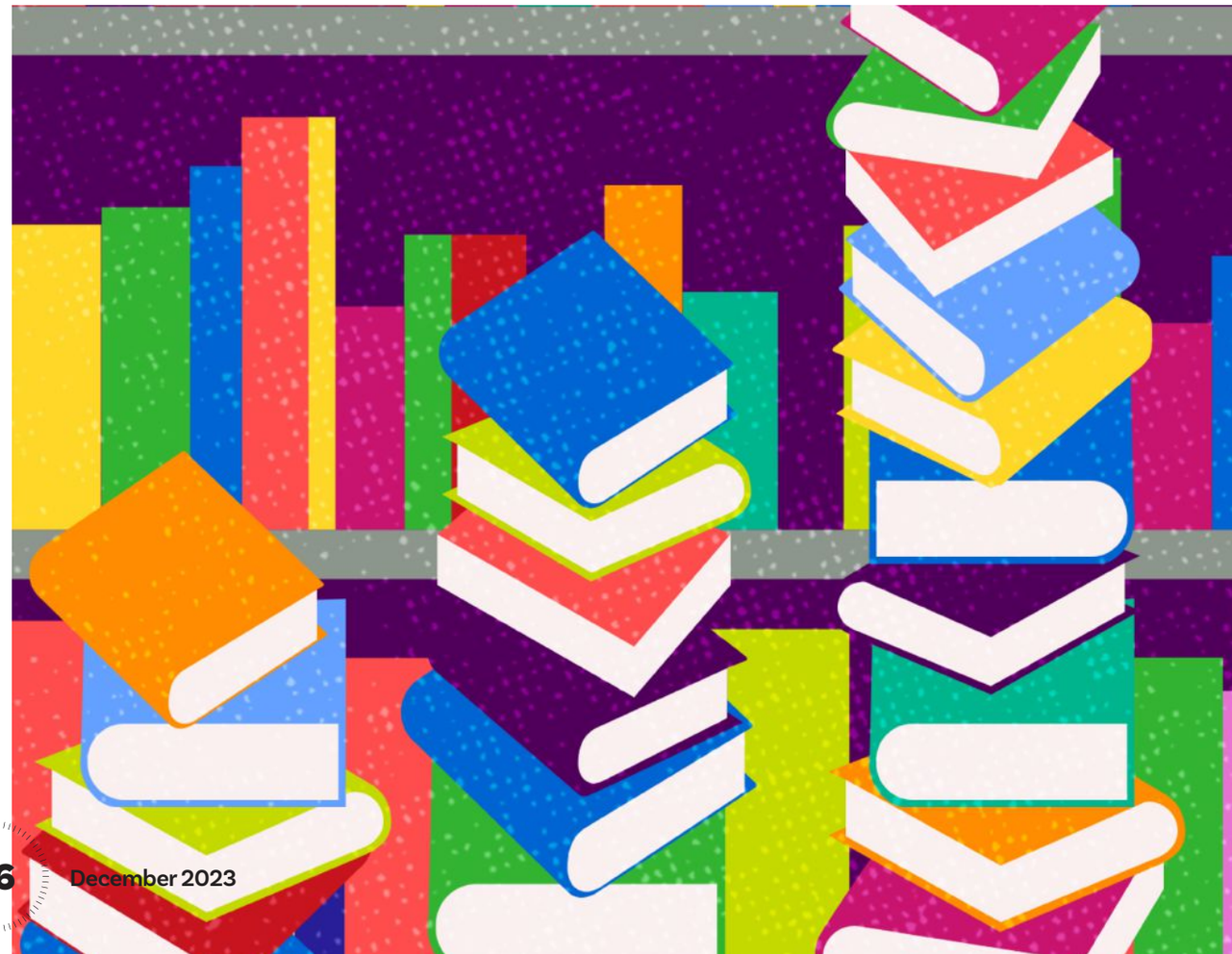
Mapping Organizational Knowledge

Some organizations use knowledge mapping to identify and visualize their knowledge. Through a depiction of collective intellectual resources, a knowledge map aims to identify the location and flow of institutional knowledge.

A good knowledge map covers tacit as well as explicit elements. The value of a knowledge map derives from its concrete visualization of information — it gives visibility to matters often understood only implicitly. It typically reveals gaps in knowledge and barriers to knowledge flows.

Information overload can be one of the challenging aspects of knowledge maps: Excessive detail and over-complication frustrate attempts to make a complex topic understandable, and readers of dense knowledge maps may not see the shape of the forest through the crowd of trees.

Conversely, as with all attempts to abstract a simple model from



complex reality, knowledge maps may generate an over-confidence in their depiction of knowledge locations and flows. The danger here is of a deceptively simplified knowledge map inadequately depicting the flow of information and expertise, hindering understanding and leading to wrong decisions.

The Social Side

The growing area of communication risks for knowledge management is crystallized in the use of social media, with risks of receiving or unwittingly disseminating disinformation and misinformation. Social media use presents risks for both categories of knowledge — with regard to the sharing of information and with the judgment and expertise required to prudently handle publicly visible knowledge.

For employees with permission to update the organization's social media sites, an error of judgment can be catastrophic. In recent months, there have been several examples of politicized marketing campaigns (promoting everything from beer to swimwear to cosmetics) that have led to reputational damage, consumer boycotts, and corporate losses.

In some cases, an organization may be willing to place its political opinions before profits, even at the risk of alienating a segment of its customers. In other cases, it is inadequate controls over expertise that have led to individual errors of judgment with serious financial effects.

Some corporate executives have tried to shift the responsibility for social media gaffes to allegedly "rogue," low-level employees. Whatever the political rights and wrongs of corporate social media messaging, the practical risks can be highly damaging.

Sometimes simply enabling a "comments" or "response" option may open the door to offensive material. An organization that allows two-way, public social media posts is granting the general public access rights to its accounts, with all-too-obvious dangers. (YouTube, for example, has a "disable comments" option to avoid such risks.) And a particularly acute social media risk arises from gaps in cybersecurity: A hacked social media site might be used to spread information that damages an organization's reputation.

There are many internal controls to protect information and expertise conveyed through social media accounts. Strict guidelines for social media use are essential, as is a clearance process to pre-authorize posts. And the continuous monitoring of social media is important to identify and eliminate posts that might slip through the authorization stage. Such measures are necessary, yet insufficient, to fully eliminate the risks. As with so much in risk management, social media risks tend to be mitigated rather than eliminated.

Maximizing Intellectual Capital

The careful navigation of knowledge management risks is crucial. The rise of social media and the ongoing digitalization of information have only added to the risks in this area. A good knowledge management culture is easier to recognize than to describe, and increasingly rests on "soft" controls like organizational culture. But by understanding the importance of both information and expertise, auditors can assist organizations in maximizing the limitless potential of their intellectual capital.

A good knowledge management culture is easier to recognize than to describe, and increasingly rests on "soft" controls.

David J. O'Regan, LittD, is auditor general of the Pan American Health Organization in Washington D.C. and the author of several books on auditing.

The New Standards are Coming

Everyone involved with this project, including the independent oversight council monitoring our due process is excited to be moving closer to completing the final product, the Global Internal Audit Standards™ which is expected to be approved this month and released in early 2024.

Stay tuned at ***theiia.org/IPPFEvolution*** *for more information.*

The Institute of
Internal Auditors

the SIPOC approach

Organizations, and internal audit, can apply quality principles to build a culture of continuous improvement and excellence.

Rachel G. Brueggen

Imagine a world where every process, from insurance to manufacturing, operates with pinpoint precision, delivering flawless results every time. In this world, defects are practically nonexistent, waste is minimized, and efficiency reigns supreme. Welcome to the empire of the Shingo Model, a transformative approach that has the potential to reshape the way organizations think about excellence and quality in every facet of their operations, including internal audit.

The Shingo Model instills a culture of continuous improvement, driving operational excellence, cost reduction, enhanced quality, improved employee morale, and ultimately, sustained competitiveness in today's dynamic markets. At the heart of the model, the pursuit of perfection meets the art of continuous improvement.

guided by principles

The Shingo Model, based on the work of Japanese engineer and scholar Shigeo Shingo, traces its origins to the renowned Toyota Production System (TPS). Shingo collaborated closely with Taiichi Ohno, a key figure in TPS, to apply the concept.

The concept evolved in response to post-World War II challenges, fostering Toyota's rise to automotive dominance. The model aims to eliminate waste, enhance quality, and boost efficiency in manufacturing and beyond. Key concepts include: *jidoka*, or automation with a human touch; just-in-time production; and *kaizen*, or continuous improvement.

The Shingo Model is globally recognized as a blueprint for operational excellence in diverse industries, emphasizing a culture of relentless improvement and customer centricity. It is built on a set of core principles that are instrumental in achieving operational excellence. Among those principles are:

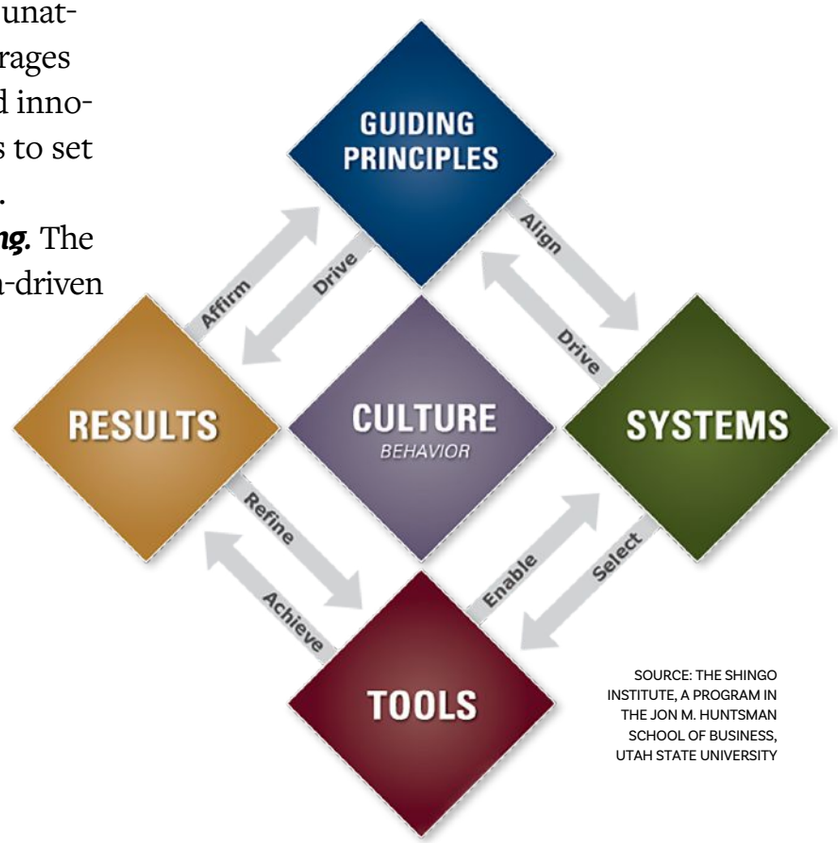
Respect Every Individual. Central to the Shingo Model is the belief that all employee contributions are valuable and integral to organizational success. Treating individuals with respect and empowering them to contribute to the organization's success creates a more engaged and motivated workforce.

Lead With Humility. Effective leadership is characterized by humility and a willingness to listen, learn, and support employees. Leaders who embody these qualities can inspire their teams to pursue excellence.

Seek Perfection. The pursuit of perfection is a fundamental principle. While perfection may be unattainable, striving for it encourages continuous improvement and innovation, pushing organizations to set and achieve higher standards.

Embrace Scientific Thinking. The Shingo Model promotes a data-driven approach to problem solving and decision making, encouraging organizations to base their actions on evidence and facts rather than assumptions.

Flow and Pull Value. Efficient processes that minimize waste and deliver value are central to the model. Implementing "flow" and "pull" concepts streamlines operations, reduces costs, and enhances customer satisfaction. The idea is to create a continuous and smooth production flow based on customer demand. Flow is the ability to create efficient workflows where the work moves from one department to another without unnecessary stops or re-work. On the other hand, pull is where customer demand drives



SOURCE: THE SHINGO INSTITUTE, A PROGRAM IN THE JON M. HUNTSMAN SCHOOL OF BUSINESS, UTAH STATE UNIVERSITY

The Shingo Model instills a culture of continuous improvement, driving operational excellence, cost reduction, enhanced quality, improved employee morale, and ultimately, sustained competitiveness in today's dynamic markets.

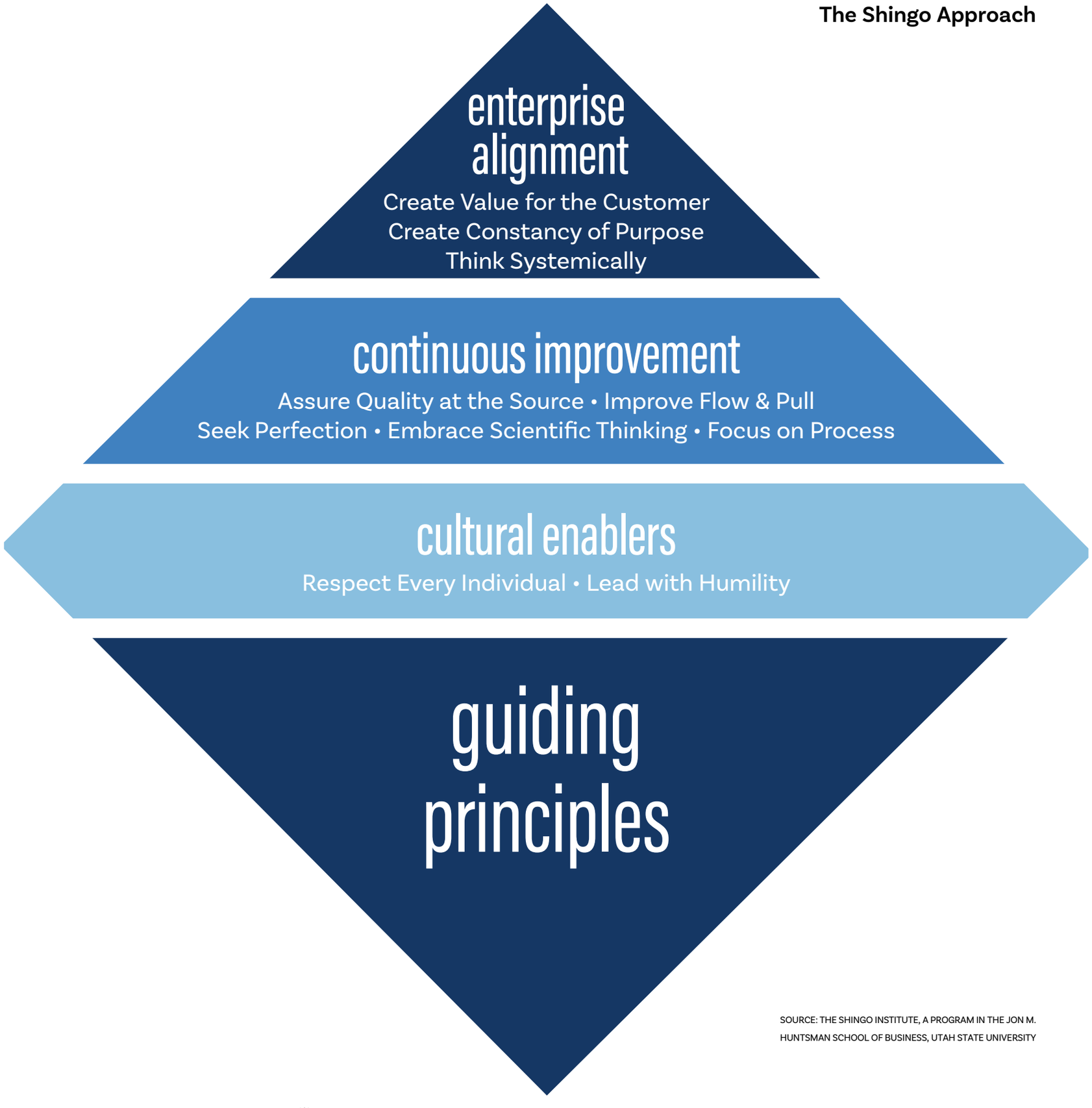
production thereby minimizing excess inventory. Together these activities allow organizations to streamline production processes, reduce waste, and more quickly respond to customer needs.

These principles not only drive operational excellence but also foster a culture of continuous improvement and innovation, making organizations more adaptable and competitive in today's aggressive business environment (see "Guiding Principles" on this page for the complete principles).

aligning with objectives

To align Shingo Principles with specific business objectives, organizations must start by defining clear, measurable, and achievable goals. Business objectives often revolve around increasing profitability, enhancing customer satisfaction, improving product quality, and reducing operational costs. When aligning these objectives with the Shingo Principles, it is essential to consider how each principle can contribute to achieving these goals.

For example, if a business objective is to reduce operational



SOURCE: THE SHINGO INSTITUTE, A PROGRAM IN THE JON M. HUNTSMAN SCHOOL OF BUSINESS, UTAH STATE UNIVERSITY

costs, aligning with the Shingo Principles might involve:

- Implementing Lean concepts to eliminate waste in processes.
- Respecting every employee's input to identify cost-saving opportunities.
- Leading with humility to encourage employees to share ideas.
- Seeking perfection by continually optimizing operations.
- Embracing scientific thinking to analyze data for cost-reduction opportunities.
- Focusing on flow and pull value to reduce excessive inventory.

Not all business areas will benefit equally from the application of the Shingo Principles. To identify where the principles can have the most significant impact, organizations should conduct a thorough assessment of their operations that considers factors such as current performance metrics, customer feedback, employee engagement, and the competitive landscape.

For example, if a manufacturing company receives consistent customer complaints about product defects, applying Shingo Principles to the production process is critical. By focusing on reducing defects and enhancing product quality, the company can align with the seeking perfection principle to improve customer satisfaction, thereby positively impacting its business objectives.

shingo and internal audit

Successfully embedding Shingo Principles in day-to-day internal audit engagements can be broken down into the four stages of the audit process.

Audit objectives and scope. Internal audit can align audit objectives with Shingo Principles, focusing on areas such as waste reduction, continuous improvement, and respect for individuals. And by aligning with the seek perfection principle, internal audit can evaluate how well processes adhere to Lean principles and identify bottlenecks, excess inventory, and activities that do not add value. Considerations include:

- How do managers ensure employees understand departmental objectives and the intended outcome?
- Are standards and processes measured and aligned to departmental and company goals?

success stories

In today's competitive business landscape, achieving operational excellence is paramount for sustainable success. Adopting Shingo Principles offers organizations an array of advantages and benefits, with improved quality, efficiency, and customer satisfaction emerging as notable outcomes.

enhanced quality. Shingo Principles emphasize a deep commitment to quality in all aspects of operations. Fostering a culture of continuous improvement and error prevention can lead to higher quality products and services.

Case Study: Toyota, a pioneer in implementing Shingo Principles, has consistently delivered high-quality automobiles. Its commitment to quality has not only reduced recalls but also earned the company a reputation for reliability and durability. The Toyota Camry has consistently been one of the top-selling sedans in the U.S. for several years.

employee engagement. Shingo Principles promote a culture of respect and encourage employees to actively participate in continuous improvement efforts. Engaged employees are more committed and motivated, leading to increased productivity and innovation.

Case Study: Johnsonville Sausage empowered employees to make decisions about their work at the moment a defect or error was identified. According to *TWI Case Studies, Standard Work, Continuous Improvement, and Teamwork*, by Donald Dinero, this led to a 30% increase in productivity and a significant reduction in employee turnover.

Audit techniques and execution. Internal audit should examine the organization's culture regarding continuous improvement, including kaizen events and Plan-Do-Check-Act cycles. Auditors can evaluate how well the organization fosters a culture of continuous improvement and identify areas where this culture can be strengthened. Considerations include:

- Reviewing value stream mapping with departments to understand the "why" behind processes and metrics and not just the "how."
- Determining whether there is a platform for associates to communicate improvement opportunities or raise the flag to prevent errors.

Resource and knowledge management. Internal audit can incorporate gemba walks (i.e., the place where value is created) into the audit process to observe processes in action and engage with employees on the job. Auditors can use these walks to identify opportunities for process optimization while gathering perspectives and feedback on how employees are involved in decision-making and problem-solving. Considerations include:

- Does the organization engage in lessons learned and sharing knowledge?
- Are team members included in process improvement discussions?
- Are upstream and downstream impacts considered?

Reporting and issues management. Internal audit should document audit findings, observations, and recommendations clearly and comprehensively, emphasizing their alignment with Shingo Principles. It should then track the progress of audit findings over time to determine the effectiveness of process improvements and share learnings throughout the business. Considerations include:

- Does the business consider the impact and value to customers when mitigating findings?
- Are the right performance measures in place to track behaviors?

Internal auditors can build powerful, cross-collaborative relationships throughout the organization. The opportunity to co-create with departments can help solve systemic

success stories continued

increased efficiency.

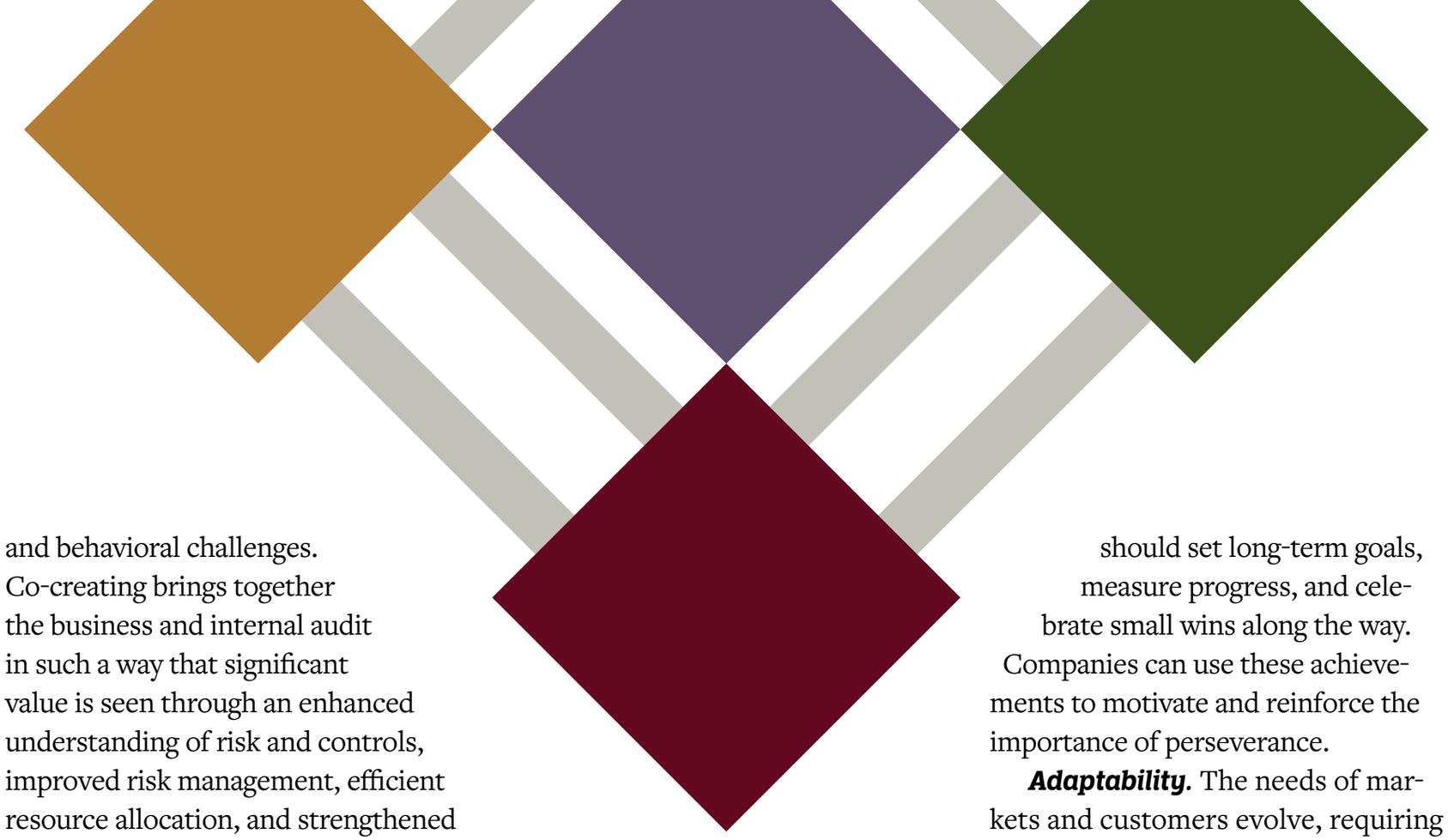
Shingo Principles promote Lean thinking and the elimination of waste from processes. This leads to streamlined workflows, reduced lead times, and optimized resource use, all of which contribute to operational efficiency.

Case Study: According to the *TWI Case Studies*, furniture manufacturer **Herman Miller** applied Shingo Principles to its production processes, resulting in a 50% reduction in lead times, a 20% increase in labor productivity, and a significant reduction in waste, ultimately leading to cost savings and higher profitability.

competitive advantage.

Organizations that adopt the Shingo Principles often gain a competitive edge. They can respond more effectively to market changes, adapt to evolving customer preferences, and innovate faster than their competitors.

Case Study: Wiremold, a manufacturer of electrical wire management systems, achieved remarkable success by implementing Shingo Principles. According to *Better Thinking Better Results: Case Study and Analysis of an Enterprise-Wide Lean Transformation*, by Bob Emiliani, David Stec, Lawrence Grasso, and James Stodder, the company reduced lead time from eight weeks to one day, increased on-time deliveries from 70% to 98%, and boosted profitability significantly, making the company a market leader in the industry.



and behavioral challenges. Co-creating brings together the business and internal audit in such a way that significant value is seen through an enhanced understanding of risk and controls, improved risk management, efficient resource allocation, and strengthened accountability of risk ownership — all of which promote transparency and improved stakeholder confidence.

overcoming challenges

Implementing Shingo Principles can be a transformative journey for organizations, but it has its challenges. Perseverance and adaptability are key to overcoming common obstacles.

Resistance to change. Employees may be resistant to changes in their established routines. Organizations can engage employees in effective change management, communicate the benefits of Shingo Principles, and involve them in the decision-making process. Companies can show how these principles will make employees' work more meaningful and satisfying.

Lack of leadership commitment. Without strong commitment, Shingo Principles cannot take root. Organizations can develop leadership through training and coaching to ensure leaders understand and embrace the principles. Leaders should be held accountable for driving the change.

Short-term focus. Organizations often struggle to maintain momentum beyond initial improvements. They should set long-term goals, measure progress, and celebrate small wins along the way. Companies can use these achievements to motivate and reinforce the importance of perseverance.

Adaptability. The needs of markets and customers evolve, requiring organizations to adapt continuously. Adaptability should be made a part of the organizational culture. Employees should be encouraged to seek out and respond to changing conditions by applying Shingo Principles to swiftly improve processes.

Resource Constraints. Limited budgets or resources can hinder implementation efforts. Initiatives should be prioritized based on their potential impact on business objectives. Organizations can start small, build momentum, and reinvest savings into further improvement projects.

Complacency. As organizations see initial success, there is a risk of becoming complacent. They should encourage a culture of continuous improvements, where employees are always seeking ways to enhance processes and performance.

To overcome these challenges, organizations must learn from them, adjust strategies, and persist in efforts to create a culture of excellence that aligns with the Shingo Principles.

the path to excellence

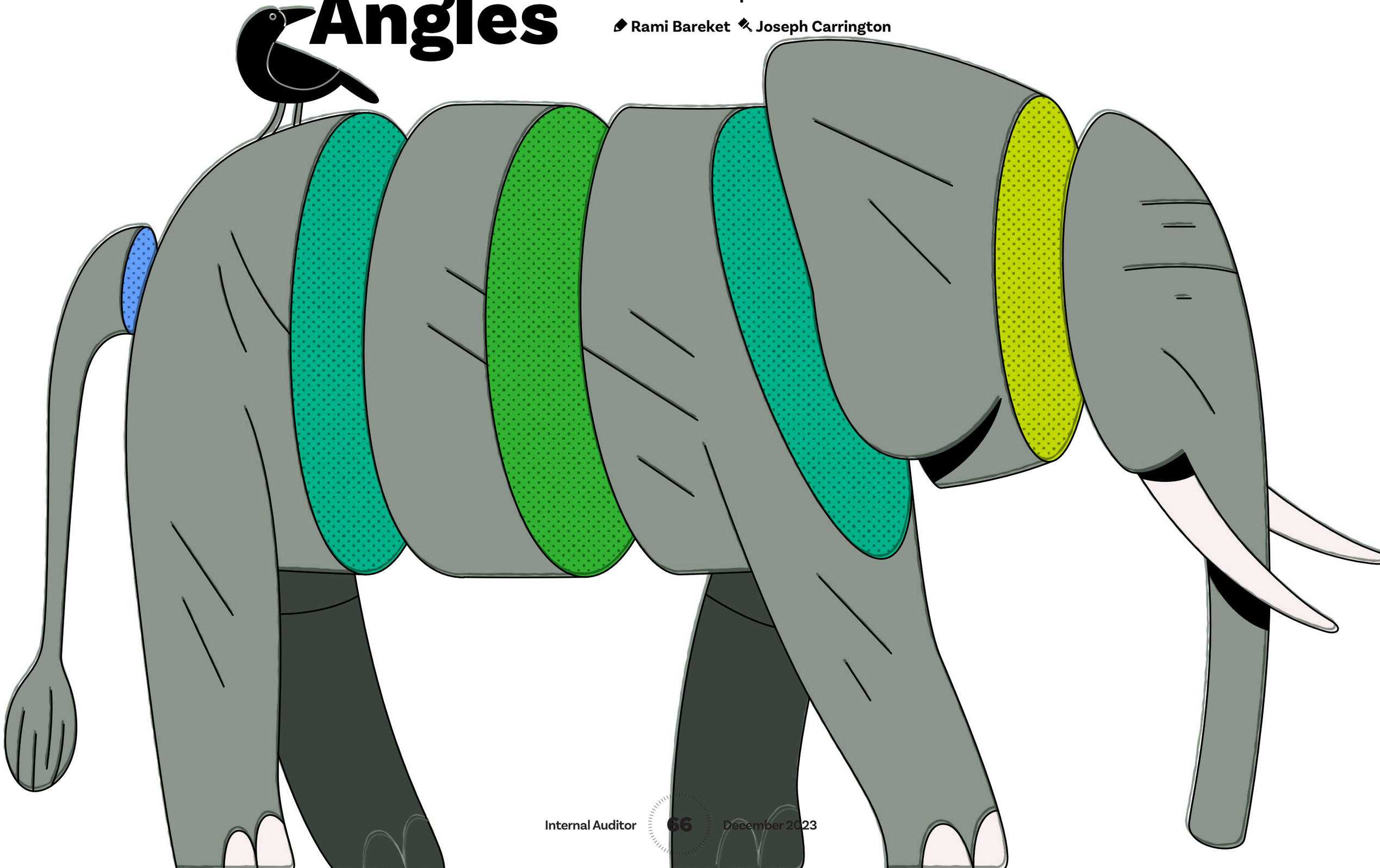
The Shingo Model encapsulate a powerful framework for achieving operational excellence and driving continuous improvement in modern business operations. In today's rapidly evolving business landscape, the principles empower organizations to remain agile, responsive, and competitive. By fostering a culture of respect and continuous improvement, companies can adapt to changing market demands, reduce costs, improve quality, and enhance customer satisfaction. The Shingo Model offers a proven path to operational excellence, ensuring that businesses thrive today and in the future.

Rachel G. Brueggen, CIA, CRMA, is an audit practitioner in Florence, Ky.

From All Angles

Process-mining tools provide internal auditors with broad and in-depth information about business processes and controls.

Rami Bareket Joseph Carrington



When auditing a business process, understanding the process is crucial. In traditional audits, auditors rely on interviews with audit clients to comprehend the business process, often requesting examples from system records, reports, and documents.

The rapid development of artificial intelligence, machine learning, and process-mining technologies is offering a more comprehensive solution for internal auditors. By harnessing advanced tools, internal auditors receive broad, in-depth information about business processes and controls during their risk assessment, enabling them to better understand the processes and make audits more efficient.

Process-mining tools examine business processes by probing the transactions entered and generated within a system. They use this data to construct a flowchart of the process's workflow, which provides insights into the various transaction workflows taken in the process and highlights the different operations and steps performed in each workflow. Additionally, the tools provide statistical information, such as transaction volumes and their proportions within each operation or stage.

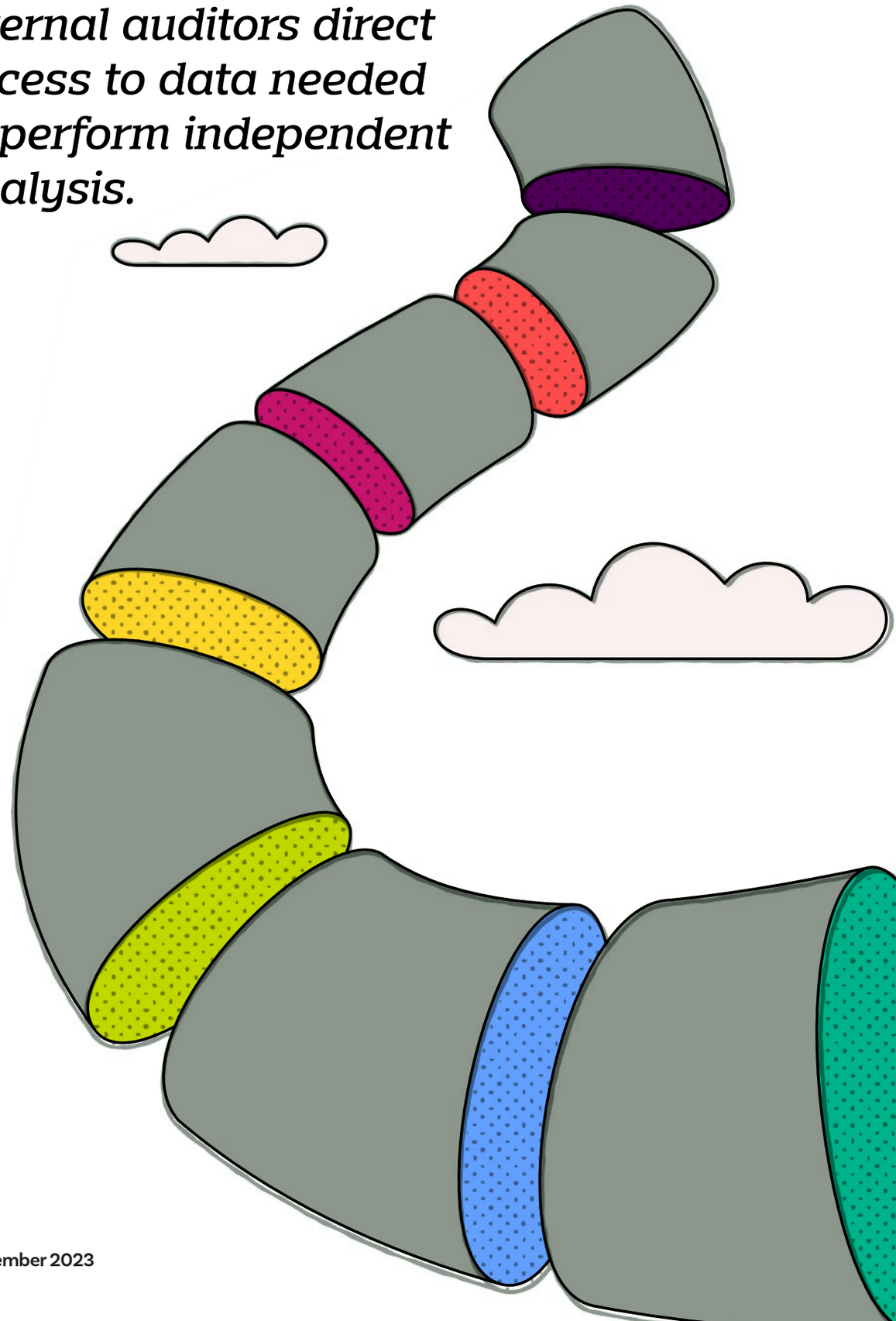
Streamline Audits

Using the process-mining approach, internal auditors gain an understanding of the business process and its constituent actions and phases before interviewing the client. Armed with this knowledge, auditors can focus on asking qualitative questions related to the data, actions, and phases within the process. They can explore the reasons behind differences among workflows — particularly those less commonly taken — leading to more insightful audit discussions.

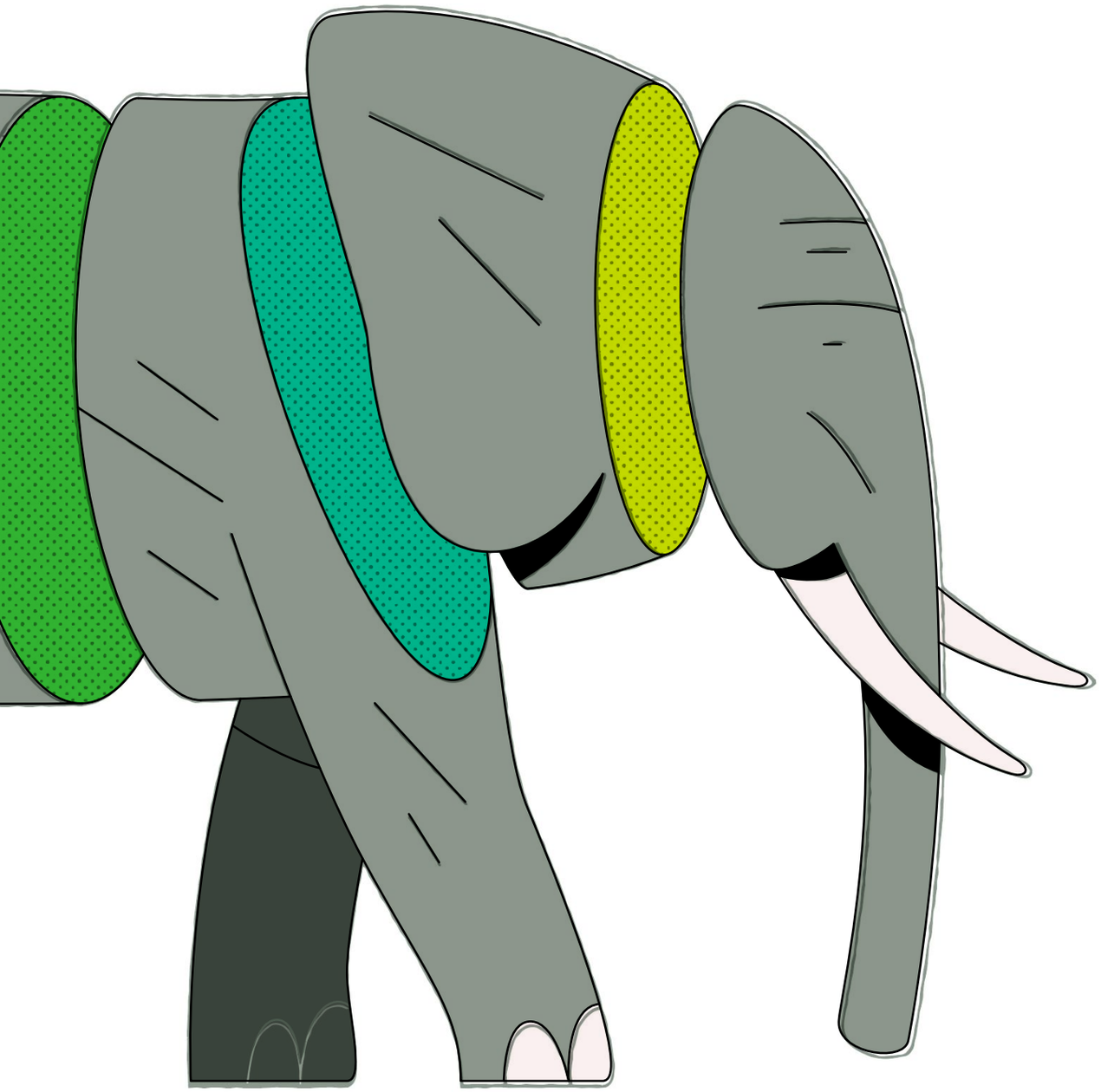
Advanced tools give internal auditors direct access to data needed to perform independent analysis. In the past, auditors needed to request data from the business unit, which required assistance from IT personnel. Then the auditor would need to verify that the data was accurate, which was time-consuming and error prone.

Advanced tools streamline the gathering of data. The auditor has immediate access to the necessary data, which saves time, reduces the potential for errors in data retrieval, and ensures data integrity.

Advanced tools give internal auditors direct access to data needed to perform independent analysis.



Modern auditors now enter engagements equipped with comprehensive insights about the business process under review.



Improved Efficiency. Advanced audit tools enable audit teams to be more efficient and shorten audit times. Where past auditors approached their tasks without prior knowledge, modern auditors now enter engagements equipped with comprehensive insights about the business process under review. The tools provide a clear understanding of the various workflows within the process, including those that are less commonly followed. Additionally, auditors have access to detailed data and statistics related to the business process.

For example, auditors can quickly access key metrics such as the total number of suppliers engaged, the number of new suppliers added in a given year, and the annual expenditure associated with procurement activities. Armed with this knowledge, auditors can efficiently focus their efforts on areas of high importance and potential risk, optimizing their audit approach and ultimately enhancing the effectiveness of the audit process. An example is focusing on purchases from suppliers that have increased substantially over one year compared to purchases from other suppliers for the same goods or services.

Another audit application is examining complex contracts with suppliers in which substantial additions have been made to the agreement over several years. Focusing on such high-risk areas can enable audit teams to deliver more insightful audits.

Enhanced Analysis and Comparison. Organizations with multiple subsidiaries often use several different enterprise resource planning (ERP) systems. Internal auditors can use advanced tools to perform comprehensive analysis and compare business processes and data across their various entities and ERP systems.

This approach enables auditors to efficiently analyze and compare business processes to identify similarities, differences, and areas for improvement across the organization's subsidiaries (see "Workflow Analysis" on page 69). By centralizing this analysis, companies can streamline their operations, enhance consistency, and establish best practices throughout the organization.

This capability gives internal auditors a holistic view of the organization's operations, which produces better insights, data-driven decision-making, and enhanced coordination among an

organization's business units and subsidiaries. Ultimately, these gains can improve organizational performance and competitiveness.

Maximize Monitoring

As use of process-mining tools continues to grow within internal audit, organizations should consider when and how to hand the tools over to other assurance functions. For example, should they be used by the compliance and risk management functions of the second line, the managers of the business units in the first line, or both?

The answer to this question depends on various factors, including the organization's maturity level in using advanced tools, the driving force behind their adoption, and the power dynamics within the control environment. One approach is for the second line to be responsible for using the tool for continuous monitoring and control, while internal audit evaluates how those functions use the tool, including verifying that users check and address all exceptions that have arisen.

By carefully considering the organizational context and aligning the use of process-mining tools with the appropriate stakeholders, organizations can maximize the tool's benefits and effectively navigate the complexities of their control environment.

Detect Anomalies

In addition to examining processes, internal auditors can use advanced tools to monitor, analyze, and detect anomalies in business transactions. Such testing can encompass evaluating the adequacy of the defined base rules, examining how the business monitors and addresses exceptions, and assessing whether the organization learns from past experiences to drive improvements. To obtain the most accurate results, auditors should follow some guiding principles.

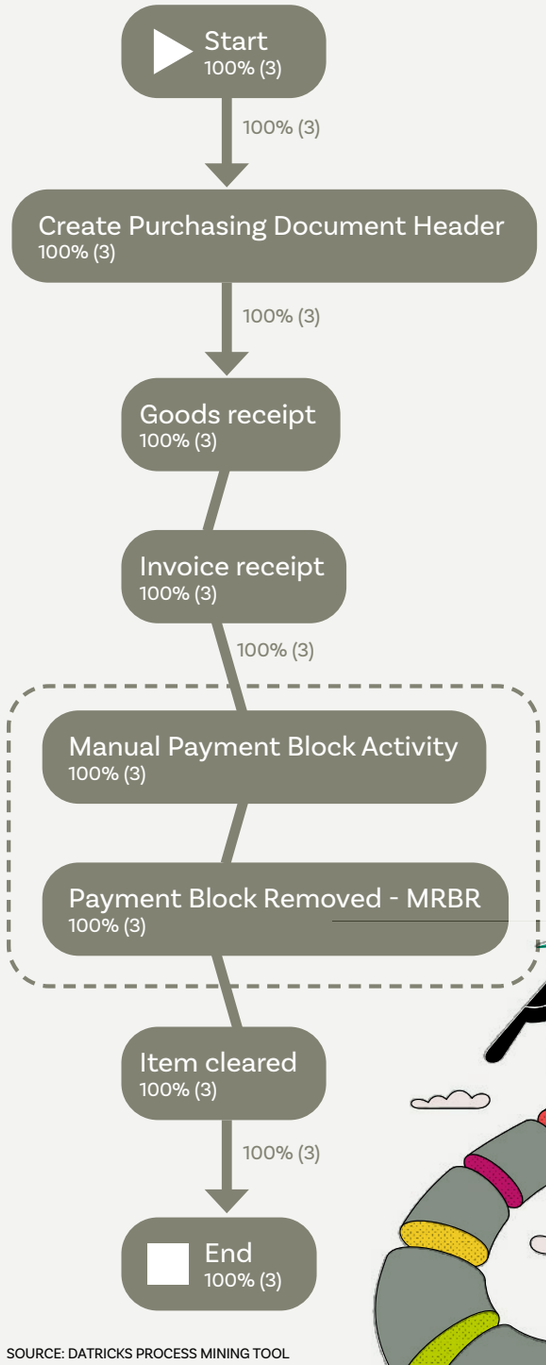
Establish a direct connection to the production database. This connection to financial ERP, sales, human resources, and other systems makes it easier for auditors to retrieve and extract data. It is essential to ensure both quick response and retrieval times, while avoiding any negative impact on the production system such as slowing down response times or disrupting existing users. Striking the right balance is crucial to maintain system performance and user experience.

Workflow Analysis

Advanced tools can help internal auditors overcome challenges analyzing business processes in complex organizations. An example is comparing the procure-to-pay workflows for a global company with subsidiaries running multiple enterprise resource planning systems. In the flowchart on the right, auditors can observe two distinct workflows.

1. **Manual payment block.** This workflow features a manual hold on the payment to the supplier, while the company validates the accuracy of the payment. The company releases payment once validation is completed.
2. **Payment block removed.** In this workflow, the ERP system checks the validity of the payment automatically and payment is made after it is verified.

Auditors should focus on understanding the rationale behind cases where a manual blocking operation and subsequent manual release are performed, as opposed to cases where the release occurs automatically. By investigating these variations, auditors should aim to understand the factors that influence the choice between manual and automatic payment processing.



SOURCE: DATRICKS PROCESS MINING TOOL

Define base rules. This comprehensive list of rules is designed to identify exceptions or anomalies. In the context of internal auditing, it serves as a checklist based on best practices specific to the business process being examined.

For example, base rules in the procurement process include identifying instances where a supplier is duplicated in the master data, detecting duplicate payments made to suppliers, and flagging cases where a supplier's bank account branch is located in a different country. These rules help ensure the accuracy and integrity of the audit process by highlighting irregularities or risks.

Minimize false-positive cases. A weakness of some analytics tools is that they flag many anomalies, but a large percentage of them are false positives. That is beginning to change as internal auditors begin to use AI and machine learning tools to identify and eliminate false-positive cases. Leveraging these tools in tandem with fine-tuning the base rules can further lower false positives.

It is important to acknowledge instances where tools fail to detect suspicious movements or transactions during data retrieval. When this happens, auditors won't know about these problems.

Ensure the tool investigates anomalies effectively. For example, internal auditors could investigate a suspicious invoice using a tool that enables them to drill down to the granularity of the billing-line level. The tool also could display all invoices from the same supplier with identical billing information and provide other relevant details the investigator requires. Such capabilities significantly facilitate the investigative process, reducing the time required for investigations and enhancing trust in the tool.

Select an intuitive interface. Just like any other software, advanced audit tools should have a user interface that provides the functionality users need and is easy to use.

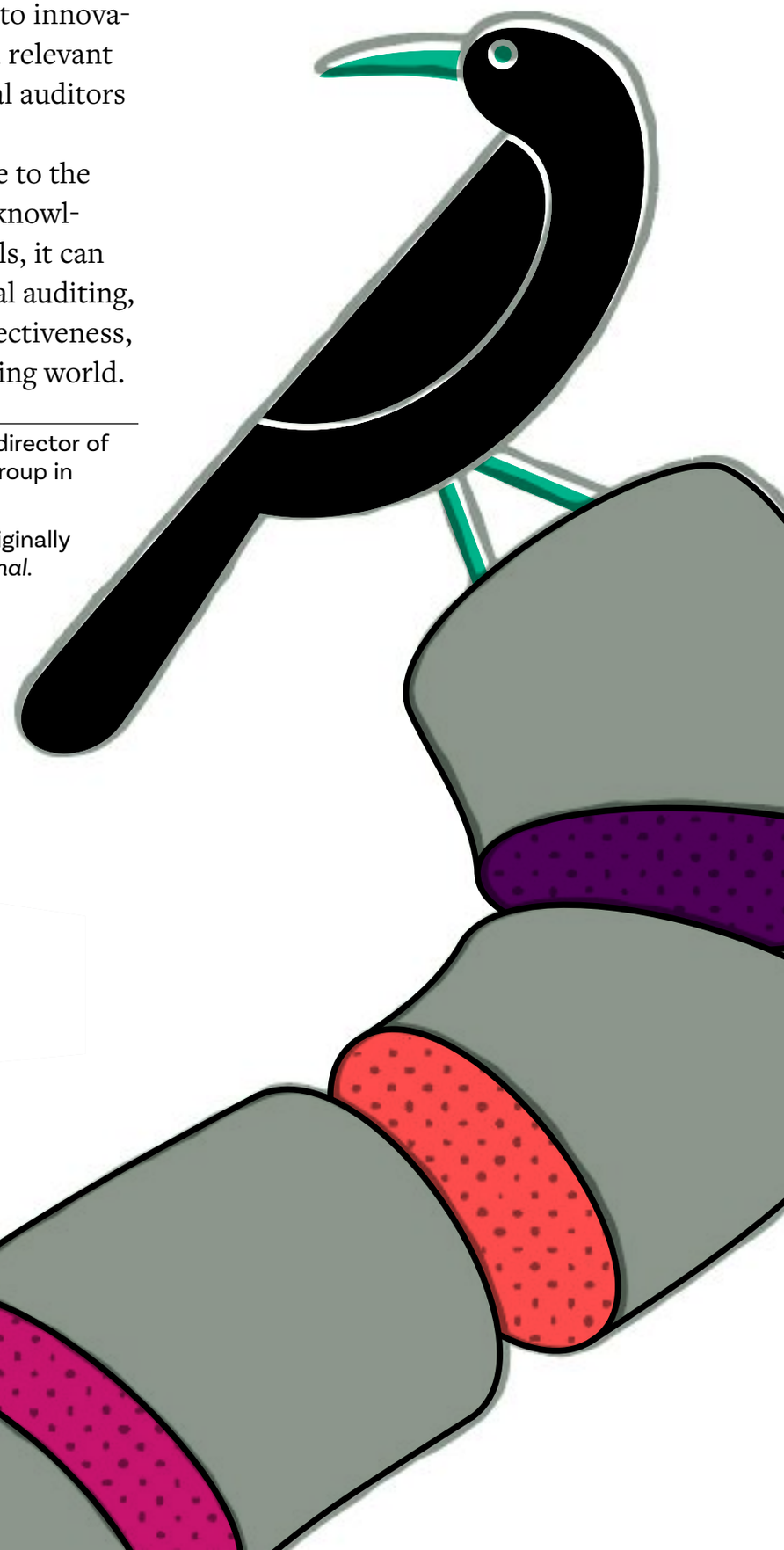
Empowered Through Technology

As groundbreaking technology rapidly transforms the world, internal audit must adapt and leverage advanced tools to elevate the quality, efficiency, and optimization of audit work. Using these technology solutions effectively requires an unwavering commitment to innovation and progress from all relevant stakeholders, with internal auditors at the forefront.

Internal audit must rise to the occasion. Empowered by knowledge and cutting-edge tools, it can shape the future of internal auditing, ensuring its relevance, effectiveness, and value in an ever-evolving world.

Rami Bareket, CRISC, CISA, is director of the internal audit unit at ICL Group in Beer-Sheva, Israel.

A version of this article was originally published in the *IIA-Israel Journal*.



Learn. Earn. Report. Retain.

Make your certification stick!

Now is the time to keep your esteemed certification active by earning and reporting CPEs to meet this year's guidelines (and prove value and credibility).

Report CPEs by 31 December. *theiia.org/CPE*

The Institute of
Internal Auditors

A State of Resilience

Internal auditors in Lithuania are showing resourcefulness in the face of major disruption.

Audra Nariunaite Grace Lanksbury

The world has seen significant upheaval over the last few years. The global pandemic reshaped many areas of life, particularly in the business world. There have been new geopolitical conflicts too, including Russia's invasion of Ukraine on Feb. 24, 2022. For Lithuania and other Eastern European countries, a war taking place just beyond their borders has heightened tensions and ushered in a period of uncertainty.

The recent global events are forcing companies to assess risks not only from a growth perspective, but from a divesting perspective. In Europe, international companies have had to adjust how they view risks to their operations in countries sharing borders with global superpowers. It has added a worst-case scenario of "having to shut down a business in country X" to long-term strategic planning discussions.

Like many of its neighbors, Lithuania is no stranger to geopolitical conflict. With a population of nearly 2.8 million people and a history spanning over a thousand years, Lithuania has weathered countless trials and remains resilient. Even with the omnipresent news of war, there is a semblance of normalcy in everyday life. The flexibility ingrained during the pandemic has, in many ways, equipped businesses and professionals to quickly adapt when faced with fresh challenges.

Like their country, internal auditors in Lithuania have responded to this latest upheaval with resilience and pragmatism. Auditors have helped guide their organizations around new risks and challenges, and their experiences can serve as a lesson for internal auditors undergoing similar change and upheaval.

A Time of Disruption

The Russia-Ukraine war has created multiple challenges for organizations and internal auditors in Lithuania, including complying with numerous international sanctions. These external impositions have forced businesses to take a closer look internally, reviewing processes related to anti-money laundering, sanctions observance, Know Your Business/Know Your Customer (KYB/KYC) regulations, and third-party risk assessment. Sanctions compliance in Lithuania means not only observing European Union (EU) sanctions, but also following changes to U.S. sanctions, as the U.S. Office of Foreign Asset Control issues guidance on sanctions.

Because of its relatively small size, most of Lithuania's businesses rely heavily on imports, making it a truly global marketplace. One of the most significant changes businesses have faced is finding alternative suppliers in other countries. The sanctions have made it difficult for businesses to import goods from Russia, previously one of Lithuania's primary trading partners.

As in other EU countries, special projects within public and private companies may be funded by grants from the EU, which are governed by EU laws and regulations. How well an organization adheres to those laws can have an impact in terms of legal compliance, but also in terms of its reputation.

If a company is found to be noncompliant and funds are retracted, it may result in negative media attention. This can impact not only the business itself, but the country as a whole. For auditors in larger countries, this reality may seem like an extra layer of responsibility. While some internal auditors working for global companies feel the weight of "representing one's country," most do not have to consider how negative media attention could decrease foreign investment in one's home country.

Remaining Flexible

Internal audit departments have stepped up to support businesses in multiple ways. They have assessed the regulatory environments in new supplier countries and conducted risk assessments on their organization's ability to monitor sanctions compliance in these markets. They have reprioritized audits to support the organization's ability to adjust. Specifically, the lack of supplies from Russia and the search for suppliers or customers elsewhere has resulted in product shortages or disruptions.

Consider the internal audit team at Ignalina Nuclear Power Plant, which is undergoing an intense dismantling project. It is expected to achieve the "brownfield" end-stage by 2038, which involves rehabilitating the utility's land and buildings so the site can be redeveloped and the surrounding infrastructure can be used for economic activity. The nuclear power plant has unique infrastructure needs; as part of the dismantling project, there is an inflow of specialized tools and materials and an outflow of parts that cannot be repurposed on site but must be recycled or destroyed responsibly. To achieve this, the internal audit team had to find suppliers from a very limited set of companies that work with nuclear plants built in the 1980s.

Strict sanctions compliance led the team down a path of integrated solutions, using two third-party providers to conduct sanctions screening, and adopting a software as a service (SaaS) tool for conducting sanctions compliance globally. In searching for the right SaaS tool, the team had to prioritize a provider with granular data specific to Eastern Europe.

This scenario emphasizes a fundamental truth during times of disruption: No single approach is the solution; creating an ecosystem of specialized approaches is a must. While in some cases, a global sanctions screening tool may suit organizational needs, it is often the case that broader tools may not address the needs of the organization as the landscape changes.

Even while Lithuanian internal auditors are responding with resilience to support their organizations, they are still human and are naturally affected by the simmering conflict.

Standing Together

Even while Lithuanian internal auditors are responding with resilience to support their organizations, they are still human and are naturally affected by the simmering conflict. The recent stream of news about nuclear weapons being moved to Belarus (which borders Lithuania), seeing war refugees from Ukraine, and hearing about escalations in the war can create stress.

One of the ways internal auditors in Lithuania cope with the unknown is by fostering a sense of community. The Ignalina Nuclear

Power Plant's deep local ties enable it to be a center of community action and involvement. Built in 1980, the power plant has long been the city of Ignalina's major employer, and the surrounding area is populated by people who either work for the plant or know someone who does. Many of its employees actively support relief efforts for Ukrainian refugees, embodying a spirit of solidarity and hope.

Other organizations across Lithuania organize events that allow employees to support humanitarian efforts and represent their organizations in doing so. Many Lithuanian internal auditors participate in these initiatives, which helps build relationships with colleagues across departments. Working toward a noble common goal unites people far beyond what any traditional "team building" events could do.

Even the IIA-Lithuania affiliate exemplifies this resilience and adaptability. Its continued commitment to offering professional development avenues, both in-person and online, has enabled internal auditors to maintain their professional connections and enhance their knowledge.

The Lithuanian government also has been a supportive partner, offering businesses a pathway to collaborate with suppliers, especially in unique situations where no alternatives exist. Early on, the government established open lines of communication so that companies could easily obtain guidance.

Preparing for Change

Several key insights emerge from the experiences of internal auditors in Lithuania that can be applied to other teams facing geopolitical disruption:

- **Having a strong compliance framework is crucial.** In light of changing geopolitical events, internal auditors should assess adherence to international sanctions, anti-money laundering rules, and KYB/KYC requirements. The function should carry out thorough risk assessments, especially with third parties, and review compliance processes to ensure they meet international standards.
- **The human element cannot be overstated.** As geopolitical conflicts impact globally distributed teams on a highly personal level, leadership teams need to be mindful of the impact. Cultural sensitivity becomes more important, and supervisors need to educate themselves or seek out resources to ensure they are supporting their teams in ways that are culturally and context appropriate.
- **Collaboration between government and business can be beneficial.** Lithuania's approach to facilitating business collaborations with suppliers in a time of uncertainty is a good example. Internal auditors can help bridge this collaboration by acting as advisors for the company, but also as liaisons with government officials. This helps ensure the organization adapts smoothly to new regulatory environments while maintaining compliance.
- **Sanctions can disrupt traditional supply chains.** This can prompt businesses to find alternative suppliers. Internal auditors can help guide businesses through the regulatory challenges of new markets, ensuring compliance with international sanctions at every step.
- **Specialized tools and expertise are vital to compliance management.** The internal auditors at Ignalina Nuclear Power Plant learned that a mix of specialized tools and third-party expertise

Internal auditors can help guide businesses through the regulatory challenges of new markets, ensuring compliance with international sanctions.

may be needed to support compliance frameworks.

- **Sanctions compliance is a reputational matter.** Compliance with EU and U.S. sanctions is not just a legal requirement. Ensuring strict adherence to sanctions can help the company and the country maintain a good reputation. Internal auditors can ensure that compliance measures are in place and followed, helping to avoid negative publicity and its fallout.

Global disruption and change are happening at an accelerated pace. While many things change, being aware of familiar themes can help anchor internal auditors to a foundation that supports growth.

First, geopolitical scenarios will continue to evolve, and their impacts will be more profound. This mandates an unparalleled resilience and flexibility from businesses and internal audit practitioners. Internal audit functions must be there for the business, acting as a partner in tackling uncertainty. Internal auditors can harness their unique understanding of the organization and its risk profile to provide insights on the impact of new regulations, suggest ways to find new suppliers and third-party vendors, or even lend out internal audit staff to support other departments.

Second, risk assessments must remain grounded in both likelihood and impact. While COVID-19 and major geopolitical conflicts make it seem like those "black swan" events are becoming a trend, it is important not to over-correct. Instead, internal auditors should rationally assess the likelihood of these events occurring for their organization and location.

Third, the auditor's role as a trusted advisor is more pivotal than ever. Organizations will lean on their internal audit teams to provide leadership and clarity, especially when wading through complex internal processes. Internal auditors will need to balance their role as providers of independent assurance with the need to become more involved in the business and strengthen their relationships with key business stakeholders.

For auditors to remain at the forefront as trusted advisors, there's a clear call to action: They must make a commitment to continuous personal and professional growth. This means embracing new technologies, prioritizing lifelong learning, and proactively engaging with the global internal audit community to share and absorb new practices.

Networking has always been an essential part of the internal audit toolkit. With the faster pace of change, internal auditors can think of it as a way to shortcut learning.

Geopolitical scenarios will continue to evolve, and their impacts will be more profound. This mandates an unparalleled resilience and flexibility from businesses and internal audit practitioners.

Connecting Globally

The journey doesn't end here. The broader challenge is about fostering global connections. The IIA Chapter and Affiliates page can lead to a treasure trove of insights. The world of internal auditing offers a platform of shared experiences and collective growth, bridging divides and fostering connections across continents. Join IIA webinars; it is a way to travel the world virtually and meet interesting professionals who share many of the same issues.

The journey of internal auditors, especially in nations like Lithuania, offers a beacon of hope. It serves as a testament to human ingenuity and the indomitable spirit to persevere, innovate, and evolve, no matter the challenges.

Audra Nariunaite, CIA, CISA, CFE, CHC, is founder of Contemporary Compliance in Jacksonville, Fla. and a member of both the IIA–Northeast Florida Chapter and IIA-Lithuania.

Shop the Latest Releases

& Stock Up on Knowledge

Explore all of our featured new releases to stay up to date. Or browse our entire selection of the most comprehensive collection of practitioner-reviewed content available anywhere and everywhere you go.

Shop now.
theiia.org/bookstore

The Institute of Internal Auditors

Wanted: A Better Approach to Assessing Risks

Regulators are calling out companies for too often missing the larger dysfunction.

Matt Kelly Joshua Clark

Board directors understand that one of their primary jobs is to keep an eye on risk at the organizations they govern. Lately, however, regulators have been nudging all parties involved to take a broader view.

Specifically, the chief accountant at the U.S. Securities and Exchange Commission, Paul Munter, has published several statements over the last year or so encouraging companies and audit firms, alike, to do better at risk assessment. Too often, he said, companies dwell too much on issues directly related to financial reporting "while disregarding broader, entity-level issues that may also impact financial reporting and internal controls."

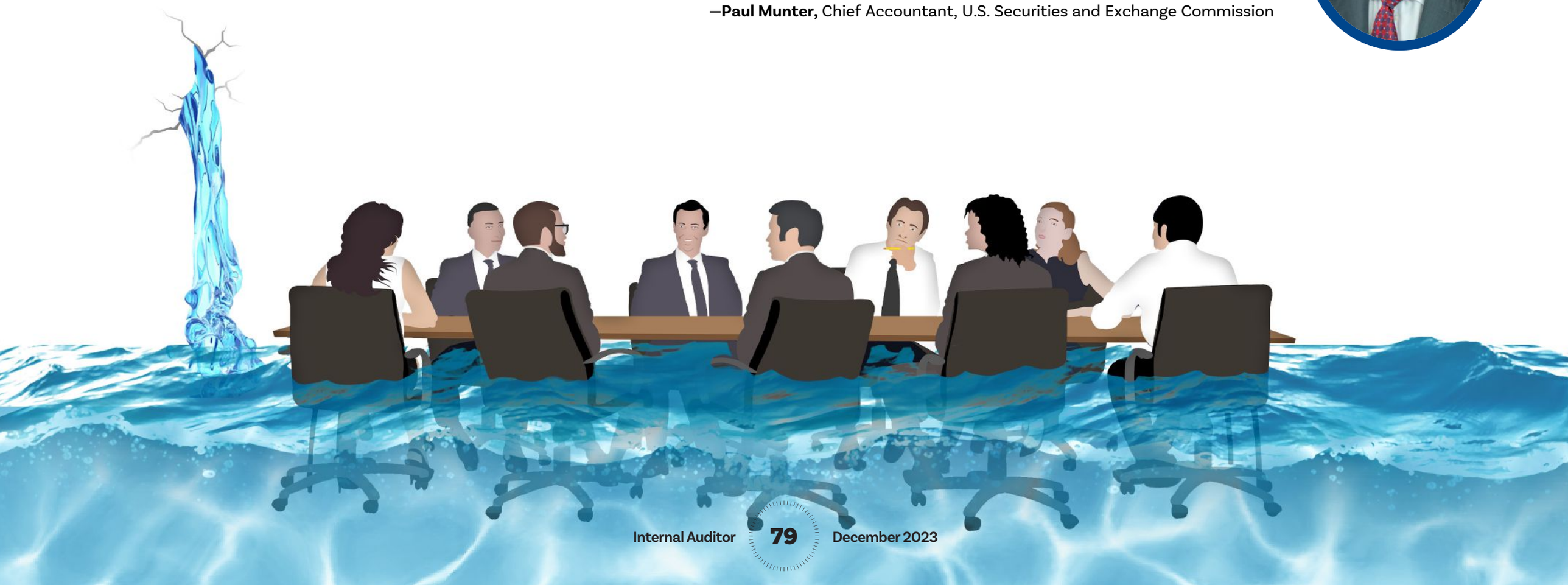
Munter's purview only extends to publicly traded companies, but he raises a point that every board and internal audit function should contemplate: How can you assure you don't get lost in the details of specific internal control failures? How can you connect the dots from a series of small incidents to catch a larger dysfunction?

That disconnect is real, says Imran Zia, director of risk management and assurance at the Vancouver Port Authority in Canada. His personal view is that too many internal auditors come from a background heavy on financial reporting (especially those who spent considerable time working at audit firms), and not enough on risk management.

"You see a misalignment in what audit is trying to focus on, versus where the business is going," Zia

Too often, companies dwell too much on issues directly related to financial reporting "while disregarding broader, entity-level issues."

—**Paul Munter,** Chief Accountant, U.S. Securities and Exchange Commission



says. "The big disconnect is, first, a good understanding of the business and the business risk; and second, really aligning your work with the business risk."

That's the pressure point, really. Regulators (and Munter is not alone here) want organizations to take a broader view of risk, finding hidden connections and root causes, so executive teams can then manage that risk more skillfully. So how do we get there?

Broader Views of Risk

Let's first look at what Munter actually said.

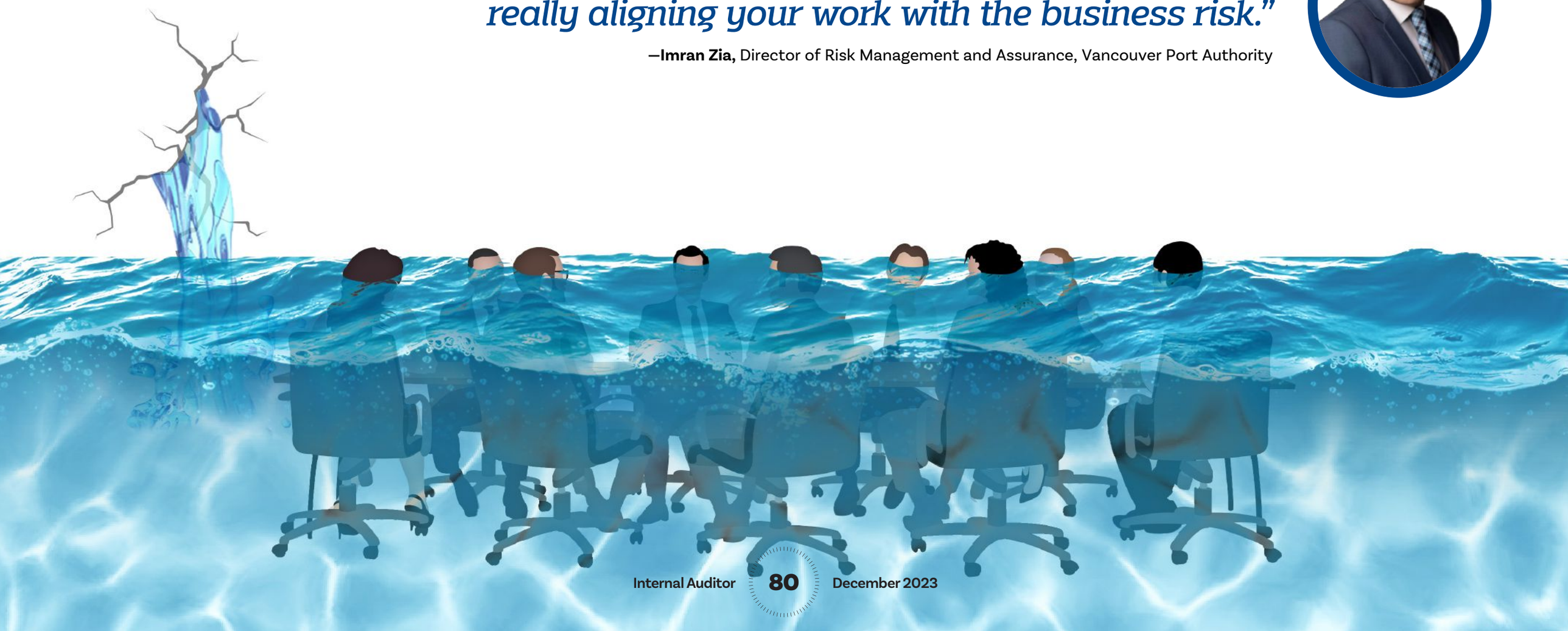
His first statement came in 2022, telling auditors that they need to do better at assessing fraud risk. Specifically, auditors need to remember that "any changes to the macroeconomic and geopolitical environment ... may result in new pressures, opportunities, or rationalizations for fraud." A thoughtful fraud risk assessment, therefore, would need to consider those larger forces.

Munter followed up with another statement published earlier this year, addressed to both audit firms and corporations, alike. It stressed the importance of taking a more comprehensive view of risk — not just the narrow question of whether a risk is directly related to financial reporting.

Some management and audit teams, Munter warned, "may be inadvertently biased toward evaluating each such incident individually or rationalizing away potentially disconfirming evidence, and conclude that these matters do not individually, or in

"The big disconnect is, first, a good understanding of the business and the business risk; and second, really aligning your work with the business risk."

—**Imran Zia,** Director of Risk Management and Assurance, Vancouver Port Authority



the aggregate, rise to the level of management disclosure or auditor communication requirements."

In other words, companies too often are looking at risk and control failures individually, rather than pausing to consider how those small incidents might add up to a larger issue worthy of informing the board or investors. They fail to see the forest for the trees.

Before you know it, that bad habit could leave boards and organizations lost in the woods. They might dwell too much on specific troublesome transactions or processes, while ignoring more systemic challenges dragging on the enterprise as a whole. Ultimately, your investors or other stakeholders pay the price for that mistake.

The wiser approach is to take that broader view of risk and internal control from the start, even if such an approach requires more governance rigor and uncovers unpleasant truths about the organization's overall ability to achieve its objectives.

The Art of Assessment

So, if the goal is a more thoughtful, comprehensive approach to risk assessment, what does that look like in practice?

The best place to start is a root-cause analysis. When issues crop up, boards need to lean on the audit team (internal and external, alike) to assure that a thorough root cause analysis has been done. Audit teams, meanwhile, need to assure that they have the skills and independence to get that analysis done, and done right.

For example, say your company has faulty financial reporting, as evidenced by improperly recording complex transactions or miscalculating the value of assets on the balance sheet. That could be caused by poor financial processes — or it might be caused by insufficiently staffed finance and accounting teams, who are overworked and making mistakes.

That's no hypothetical, by the way. It actually happened to Plug Power, a

hydrogen fuel company, that restated its financial results in 2020. Plug Power admitted in an SEC filing that it "did not maintain a sufficient complement of trained, knowledgeable resources to execute their responsibilities," and consequently, "the company did not conduct an effective risk assessment process that was responsive to changes in the company's operating environment" — exactly the sort of shortcoming Munter is talking about.

The U.S. Federal Trade Commission and other regulators have taken similar enforcement in cybersecurity. Take for example a company that suffers several small data breaches over a brief period because its employees keep falling for phishing attacks. The root cause is poor employee training on cybersecurity, which is a management-level mistake, and the company ends up with a seven-figure monetary penalty. The trick for boards and audit teams is to sniff out those enterprisewide, entity-level shortcomings before a big incident puts the company in the regulatory crosshairs.

That's not necessarily easy. The challenge is how to determine whether a series of quantitatively small errors are in fact a qualitatively material issue. For example, the IT staff might be short two out of 20 staff. That seems harmless enough, but it could lead to the company failing to implement software patches timely — a potentially huge risk.

Zia's recommendation is for audit to keep flagging those potential risks, and then putting the onus on management to address them. Tell management directly: "Hey, the aggregate impact of this could hit us bad," he says. "You need to put something in place fairly quickly to address it." Then inform the audit committee that this conversation has happened, so everyone is aware of the residual risks.

That really is the goal here: for the board, management, and audit team to have a conversation about risks, internal controls, and any shortcomings between the two. Rather than dwelling on specific control failures, talk about what those failures tell you, because that's going to say a lot about how well the organization can keep pursuing its objectives.

That's how you see the forest for the trees.

Matt Kelly is editor and CEO of Radical-Compliance.com, an independent blog about audit, compliance, and risk management.

Cybersecurity

Fraud Analytics

ESG

Data Literacy

Financial Services

IT General Controls

plusyourself

Certificate Programs with The **IIA**

Learn more · *theiia.org/PlusYourself*

David Salierno Donough O'Malley

Counting carbon isn't as easy as 1-2-3.

Sustainability isn't just a laudable goal, it's often a necessity for compliance, investor confidence, and consumer loyalty.

But even with the best of intentions, companies are finding that progress toward their goal of net zero CO2 — or beyond — is stymied by a basic problem: counting carbon. With new regulations looming, the need to develop accurate measurements is more pressing now than ever before.

This is especially true as companies look beyond Scope 1 and 2 emissions, which encompass direct emissions from company facilities and vehicles, as well as those from electricity, steam, heating, and cooling for a company's own use. Many are now setting their sights on Scope 3 — indirect emissions produced through logistics and value chains from sources not owned or operated by the company. These can include purchased capital goods, transportation, goods and services used in production, employee commuting, and leased assets — as well as downstream emissions from delivery of goods, consumer use of sold products, product end-of-life treatment, and even investments.

The intricacies of these issues occupy the thoughts of Carlos Cordon, professor of strategy and supply chain management at the International Institute for Management Development in Lausanne, Switzerland. "The challenge is that Scope 3 emissions are often 90% of the carbon footprint of a company," he says. "If you are a food company, what are the emissions of farmers who supply you and for the transport of your raw materials?"

For example, Cordon estimates there are as many as 14 steps between the farmer who grows the beans and the cup of coffee a person has with breakfast — with each step emitting CO2. "If I need to go to hundreds or even thousands of suppliers, of farmers, and they don't count their emissions, how do I estimate that?" he says.

The question is far from just academic. The answers can determine whether a company is in compliance with a growing body of regulations. It also can change the cost of its financing and affect profitability. In many ways, reducing Scope 3 emissions has become a business imperative.

Driving Forces

As public pressure for climate action increases, politicians have responded with new regulations. In 2021, the European Union (EU) passed the European Climate Law, which seeks climate neutrality across member states by 2050.

Beginning in January 2024, the EU will include maritime shipping — fundamental to most multinational operations — in its mandatory reporting requirements for greenhouse gas emissions. Shipping companies won't just have to report emissions, they'll have to buy carbon credits to offset them. Phased in over three years, the regulations require shippers to submit one European Union Allowance (EUA) for each ton of carbon emitted. These credits are purchased in the primary market through auction from the European Energy Exchange, at an estimated average cost of €90 (approximately $95) per EUA.

Cordon says these regulations, while important, aren't the only reason organizations are counting — and counteracting — their Scope 3 emissions. "A

> "The challenge is that Scope 3 emissions are often 90% of the carbon footprint of a company. If you are a food company, what are the emissions of the farmers who supply you?"
>
> —**Carlos Cordon**, Professor of Strategy and Supply Chain Management, International Institute for Management Development

second motivation is that investment funds are saying they will only invest in companies that are sustainable," he says. "The CEO of a company told me he got a letter from an investor that said, 'Given that you are not the most sustainable company in your industry, I am going to sell all my shares.'" Cordon also points out that some banks will charge businesses a lower interest rate if they are more sustainable.

Then there are the concerns of consumers who want to make sustainable purchases. The demand for sustainable products has pushed companies to reconsider their processes and reevaluate suppliers.

The Complexity of CO2 Measurement

Counting carbon isn't just useful or best practice — it could be critical to a company's survival. Yet, producing accurate results is the crux of the issue. "A farmer may be able to measure what he is emitting from his own work," Cordon says. "But what about the company that makes his fertilizer or the trucking company he relies on? They may not have the infrastructure to measure their emissions, so there's a lot of potential for mistakes."

Scope 3 also includes emissions from consumers' use of a company's products, but gauging post-purchase behavior is difficult. A detergent maker, for example, may create soap that works well at low temperatures, reducing the need to heat water to wash clothes. But are consumers actually using the product that way?

Part of the challenge for companies is while Scope 3 regulations are very precise, carbon measurement is largely based on estimates, Cordon explains. Despite significantly lowering its carbon emissions, a regulator may say a company fell short — even if it missed by a small amount.

"Sometimes there's a preference to be precisely wrong rather than approximately right," he says. For example, to demonstrate accuracy, a company may report that it emits 839,245 tons of carbon, when the imprecise nature of current measurements means it is really 840,000 tons, more or less.

The Risk of Inaction

Carlos Cordon notes there are significant risks of not moving aggressively on Scope 3 sustainability. In addition to complying with current regulation, there is a need to keep up with — and anticipate — regulatory changes.

For example, Cordon says he was recently in Madrid, where local regulations prohibit use of cars that emit a lot of carbon. "As a car manufacturer," he explains, "you might suddenly find yourself making cars that a regulator has now forbidden in parts of Europe." He adds that restrictions are likely to increase as extreme weather events raise more concern among country leaders, citizens, and regulators.

This is why many companies are examining the potential for these types of changes in their risk assessments, Cordon says. Prudent organizations will evaluate their sourcing strategies and materials used in the event there is a shift in regulation — so they aren't left unprepared.

Cordon also highlights the possibility of competitor innovation and the risk of losing market share. "Suppose another company develops a superior technology that's sustainable — if it's cost-effective and practicable, that company could take business away from, or potentially wipe out, all of its competitors," he says.

Measurable Innovations

Cordon does see progress being made toward improving measurement accuracy, pointing to innovation in the farming industry. "Satellites, drones, and Internet of Things (IoT) technology are being used for measuring, sometimes with surprisingly good results," he says. He cites a large Brazilian farming company that combines drones with IoT. "They have thousands of cows fitted with sensors to measure greenhouse gases — they're also trying to understand how certain behaviors cause the cows to emit more or less gas and make adjustments."

Cordon notes that to achieve net zero, many companies are looking outside the scope of their main business. For example, some food companies plant crops that aren't directly connected to their product but instead are meant to capture CO2. Others have invested in preserving forests, which absorb and store large amounts of carbon from the atmosphere.

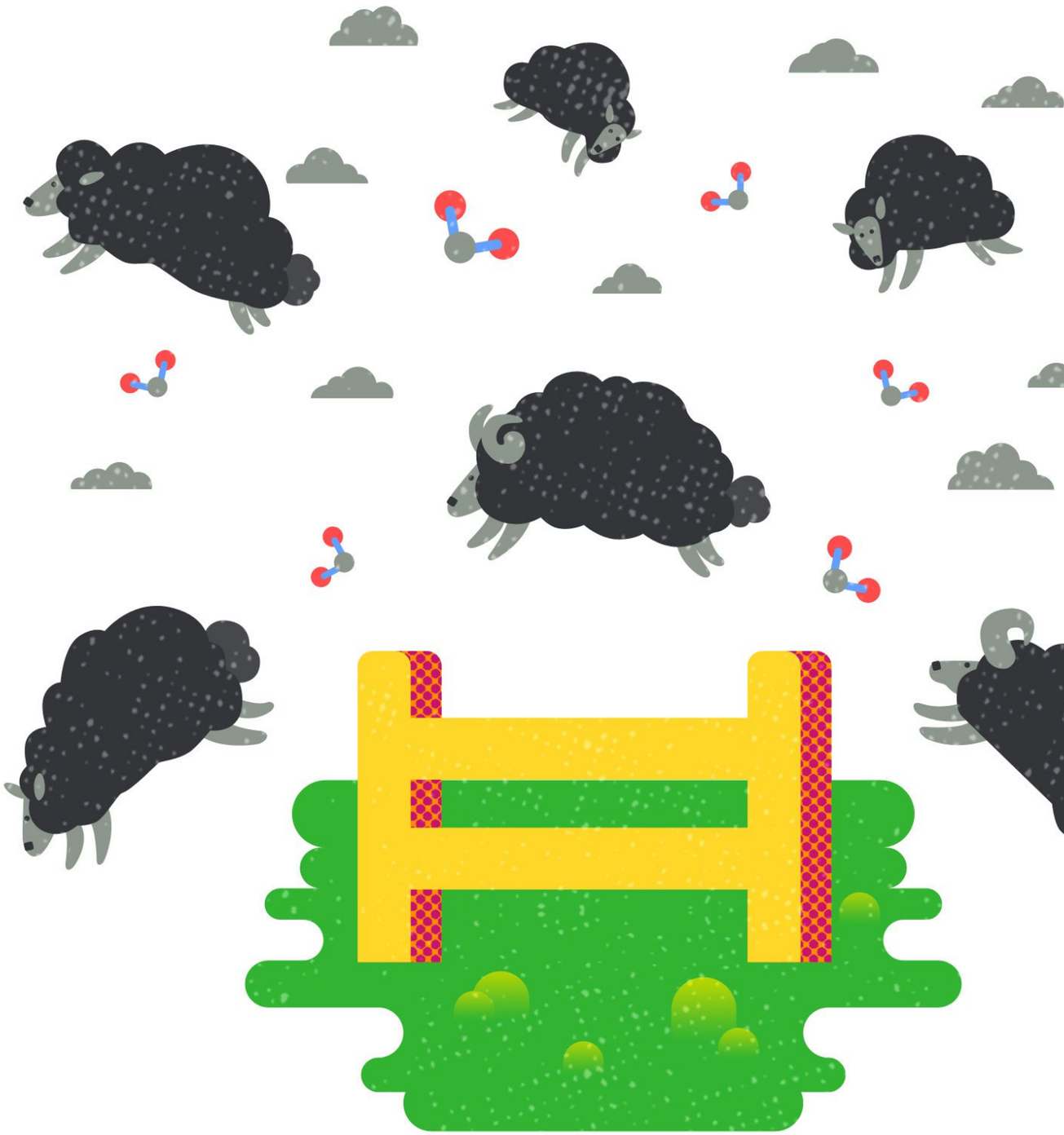
Using these techniques, certain companies are even striving to become carbon negative to address emissions from prior years, Cordon adds. These companies seek to retroactively erase their carbon footprint since they first started doing business.

"Being net negative is a great objective, but whether you can do it or not depends on the industry you're in," he says. "If you're a car company or an airline, it's virtually impossible." Cordon adds that some companies are trying carbon capture techniques, putting carbon into the soil, but the available technologies are difficult to scale — particularly for large organizations.

Carbon Control

Overall, Cordon remains optimistic about both the ability of companies to increase sustainability and the development of new technologies that can be scaled to meet organizational demands. Counting carbon accurately, though, remains a struggle, one that internal audit can assist with.

"Auditors can play a fundamental role in helping with supply chain sustainability to find out where to put the effort, pinpointing where to improve," he says. "They're well-suited to assess the risks and advise companies about where to direct resources." Cordon is optimistic about that too, predicting that, in the campaign to reduce carbon, "auditors are going to become a driving force."



David Salierno is managing partner at Nexus Content in Winter Park, Fla.

Shraddha Deokar >

Internal Audit Graduate,
University of Texas at Dallas

"**Fuel** the future of the profession."

MAKE A DIFFERENCE THAT'S NOTEWORTHY

Thanks to generous donors, the Internal Audit Foundation funds cutting-edge research, creates groundbreaking content, and supports academic programs, curriculum, grants, and scholarships to evolve the future of the profession.

DONATE NOW
theiia.org/Foundation

Internal Audit
FOUNDATION

CUTTING-EDGE RESEARCH | GROUNDBREAKING CONTENT | ACADEMIC PROGRAMS

The Weakest Link

Cybersecurity experts address the role of human behavior in security breaches.

David Burg
Americas Cybersecurity Leader, EY

How much are employees a factor in cybersecurity breaches?

People are an enormous factor in every cyber intrusion. What's most interesting about a recent surge in attack activity are the techniques being used to compromise a company. They are generally very simple and involve employees making mistakes or perhaps not following a policy or procedure, enabling the attack to proceed.

Humans want to trust. If the threat actor is representing themselves as a person that an employee trusts, then the employee may think, "This looks or sounds like my company help desk; I trust my company help desk." They don't really have their guard up completely to ask, "Is this really my company help desk calling me?" or "Is this really my manager reaching out to me?"

Another aspect is that people are very busy. It's often that employees have five windows and multiple tasks open on their computers, and they don't have their full attention on any one task. So, if something pops up in the middle of five other things, they may not even fully think about it — just quickly click 'okay' and move on to the next task.

What are the biggest risks with employees and cybersecurity breaches?

Business email compromise, one of the most common cyber incidents organizations encounter, is all about humans falling for an attacker's trick. That's basically where people, often

in accounts payable or receivable, receive phishing emails, phone calls, or text messages from attackers trying to get into their corporate email accounts.

And the reason they want to get into their accounts is so they can pretend to be that person and send emails to business partners, vendors, etc. and say, "Hey, we've switched our bank account from Chase to Bank of America. Here's our new routing number. Here's our new account number. Please make sure you send the next $2 million payment you make to us to this account."

Attackers also are contacting corporate help desk professionals to try to obtain an administrator's credentials. One of the mistakes on the help desk side are the simplistic challenge questions asked to confirm an employee's identity such as, "Who do you report to? When did you start? What's your middle name?" These data points are very easy for an attacker to determine by doing their research in advance. Once the attacker gains that privileged account, they can change configurations. And that's really where the damage ensues.

How do recent workplace trends affect the risk?

With more remote work, the vulnerabilities and the risks are increased because there's no telling what is in that environment or how that individual is working. Ensuring that the organization has the right controls and security features on devices going to and from home is a must. During the pandemic, some security breaches occurred because the corporate computer that was sent home with an employee suddenly became the family computer. Children and spouses were sometimes going to unsafe websites and picking up trojans and other malware.

Another human error is the assumption that a sophisticated technology like a cloud-based application is, in and of itself, safe and secure. There are vulnerabilities that can be exploited with various kinds of cloud applications and other emerging technologies. A misconfiguration can really create a problem.

Joe Nocera
Partner Leader, Cyber Risk & Regulatory Marketing, PwC

How does culture affect cybersecurity and employees making smart choices?

Culture has a big impact on the decisions employees make. Communication, transparency, and continuous employee education are the most important components to creating a safe, security-first culture within the organization.

It's important to create a culture of awareness and an environment where employees feel comfortable raising their hand to say they're concerned about something — whether it's their own activity or mistake or something they have witnessed.

When an organization chooses to enforce things like multifactor authentication and frequent password updating and complexity requirements but doesn't communicate with its workforce the risks and reasons surrounding these policies — they may be perceived as a burden. They may symbolize leadership's lack of trust in its employees. With transparency and communication, leaders can explain the escalating threat landscape the company is facing, the new

It's important to create a culture of awareness and an environment where employees feel comfortable raising their hand to say they're concerned about something — whether it's their own activity or mistake or something they've witnessed.

tools and technologies the organization is adopting to help build the cyber risk management program and enhance resilience, and the integral role employees play in keeping the organization safe. It flips the script from blame to collaboration, creating a culture that empowers employees to do their part to protect the organization from the inside out.

How does employee training and testing play into better cybersecurity compliance?

As attackers grow more sophisticated and their techniques more targeted, it can be difficult to identify potential threats. There are many ways to build awareness so that employees can act as the first line of defense in identifying and reporting such threats.

One technique is creating a corporate screensaver that includes messaging around phishing awareness. Many organizations also embed a phishing report element within their email systems. This can be gamified — rewarding those who identify a threat correctly with gift cards, tokens, or other incentives. Making threat detection activities engaging encourages participation and helps embed training and awareness into the culture.

Discuss with employees what they can do to protect themselves from being used as a vector and how they can detect and report potential threats. Armed with education and training, people become less of a risk to the organization and more of an asset. It keeps employees up to date on the threat landscape and the security policies and procedures they need to actively follow to report any issues. Training strengthens the cyber risk management program and results in fewer instances of phishing attacks, data leakage, and data theft.

What other controls can help mitigate the human factor in cybersecurity breaches?

Controls to implement include access monitoring tools to monitor and log employee activities and detect unusual patterns or behaviors, multifactor authentication, data loss prevention solutions to identify and prevent the unauthorized transfer of sensitive data, background checks on employees before granting access to sensitive information and systems, and a well-defined incident response plan to address insider threats quickly and effectively.

It also is important to know how to engage the organization's "insider risk" team, limit access to need-to-know information; remain sensitive to high-risk situations — such as disgruntled employees — and to discuss social media safety with the team. Partnering with the chief information security officer or chief information officer for tabletop exercises can enhance stakeholder collaboration and response processes.

Educate. Earn. Engage. The IIA's CIA Learning System is your system for success. Both a successful journey to earning the Certified Internal Auditor credential, and an exclusive invitation to a prestigious group of leaders who have your best interest in mind.

Put good, better, best to the test. ***LearnCIA.com***

THE IIA's CIA LEARNING SYSTEM®

The Institute of **Internal Auditors**

IAm

Phillip W. Hurd

With over 25 years in internal auditing, few would know I am a technologist and a "maker" (someone who visualizes a concept and then brings it to reality). I am proficient in programming, 3D printing, and laser fabrication via computer numerical control machines. 3D printing uses special plastic, metal, wood, resin, and other materials to fabricate three-dimensional objects layer by layer.

Because one's imagination is the only limit, I have used 3D printing and other skills to build solar tracking devices, hovercrafts, cutting lasers, augmented reality smart glasses, car parts, and drones. I am currently 3D-printing a high-accuracy, laser-guided telescope. Additionally, I am working on designing a 3D printer big enough to fabricate car bumpers and ground effect kits for cars. I like to keep some of the structures I make and sell the others.

Using technology daily in these creative and unique ways keeps my mind sharp and helps me visualize solutions to complex problems. I often share this thought with people I work with: Whatever the mind can conceive can be achieved.

stats

CIA, CCEP
Chief Audit and Compliance Executive
University of Houston System
Member since 2005, IIA-Houston

› Network | Benchmark | Succeed

Go **Further**

*with Executive Membership & the CAE Experience at GAM**

Access a community that facilitates distinctive professional development, the latest training, and networking opportunities, along with solutions-based, curated content and benchmarking data.

Upgrade Your Membership. ***theiia.org/Executive***

GAM WHERE LEADERS EVOLVE.

The Institute of **Internal Auditors**
Elevating Impact

**Discounted or complimentary GAM registration and VIP access.*