

HIDDEN HAZARDS
Getting to the Root of Cyberattacks

GROWTH STRATEGY
Mobilizing a Cyber Risk Plan

THINK DIFFERENT
The IIA's Global Board Chair
Suggests a Shift in Perspective

internal auditor

AUGUST 2023
A PUBLICATION OF THE IIA

A Growing Problem

As risks related to cybersecurity and AI multiply, internal audit can help untangle the threats.



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



▶ REQUEST A DEMO AT [AUDITBOARD.COM/DEMO](https://auditboard.com/demo)



Address tomorrow's risk today with Workiva.

Automate your data across the board so you can focus on the important stuff—advising the business and adding value.

Here's why thousands of audit and risk teams choose Workiva:



Insight

Easily create and pivot views to resolve the trickiest questions, and spend brain power where it matters most.



Flexibility

Tailor Workiva to fit how your team works. Change data anywhere in your risk universe, and your work will stay intact.



Automation

Workiva works as hard as you, with automatic workflows for testing, evidence requests, certifications, and more.



Centralization

Give the right access to everyone who needs it, whether you're a tester, control owner, or executive.

That's only the beginning. Learn more about Workiva at workiva.com/risk



workiva



How to successfully implement GRC software with help from control owners

GRC software can transform your organization into a risk-fighting machine that operates with ease and efficiency. But in order to be successful, everyone needs to be onboard with the new systems and processes. Without support from first line business owners, GRC software implementations are often doomed to fail.

In our checklist, we explore the six steps you need to take to ensure a successful implementation so audit teams and control owners can work together effectively.

[Download the free checklist ▶](#)



contents

Featuring

CYBERSECURITY

34

A Growing Threat

As organizations sow AI throughout the business, they risk being overwhelmed by rampant and invasive cybersecurity and privacy threats. It's a constant fight to mitigate these risks before they can do irrevocable damage.

◆ Neil Hodge



41 Hidden Depths

The asymmetry of cyber risk makes it difficult to detect what's lurking below the surface.

◆ James Bone



47 Mobilizing a Cyber Risk Strategy

Cybersecurity strategies need to address the risks introduced by digital transformation and a larger digital infrastructure.

◆ Daryl Pereira



contents

Featuring



53 Think Different

IIA Global Board Chair Sally-Anne Pitt says a shift in perspective will set the stage for internal auditing's future.

◆ Sally-Anne Pitt



59 A Spectrum of Talent

Neurodivergent employees offer many hidden strengths to organizations that are inclusive of them.

◆ Christine Janesko



67 A Case for Innovation

Canadian government auditors now have a tool to help ensure internal controls are built into innovative programs.

◆ Perla Habchi





contents

Practices

9 | **CEO Message**

11 | **Editor's Note**

13 | **Update**

CAEs are struggling to fill tech roles; some are finding success with existing employees.

17 | **Basics**

Internal auditors need insight into what DEI looks like in practice.

21 | **Tech**

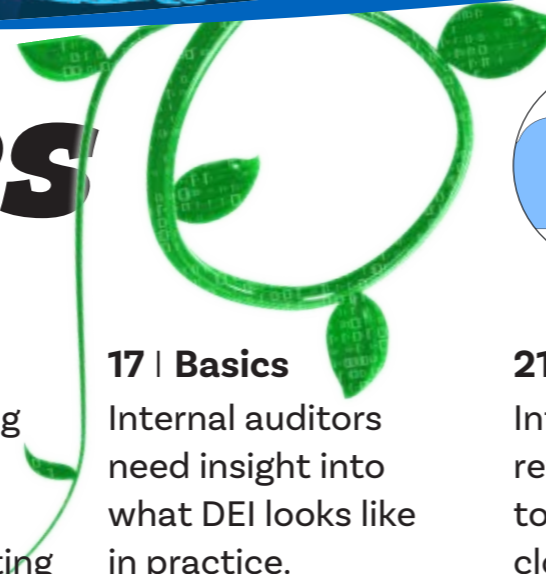
Internal audit can review key controls to help ensure secure cloud operations.

26 | **Risk**

Employee loan programs offer both risk and reward for employers.

29 | **Fraud**

A clothing store clerk fashions fictitious returns to pocket extra cash.





contents

Insights



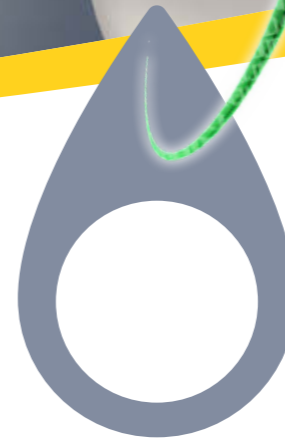
74 | Boardroom

The pressure is rising for boards to do better with fraud.



78 | The Big Idea

Why aren't helpful robots inspiring human collaboration?



84 | Viewpoints

Internal audit needs to be strategic in its approach to automating controls.



87 | IAm

Hansha Khoosy looks forward to sharing her love of travel with her daughter.

IGNITE

2023 • CONFERENCE

Where Internal Audit Leaders Emerge

The Hottest Ticket In Town & Online

Rise to the challenge, conquer the next crisis, and tap into the necessary network and tools you need to succeed. Join us at IGNITE, “Where Internal Audit Leaders Emerge.” This immersive experience will provide a real community and real-world solutions to prepare you for the ever-evolving role of a leader.

Members save \$300 when registering by August 29, 2023.

OCTOBER 24-26, 2023 • THE MGM GRAND, LAS VEGAS

REGISTER TODAY! theiia.org/ignite



The Institute of
Internal Auditors



ce message

Cyber- security in the Digital Age

In an era marked by rapid digital transformation, cybersecurity threats loom over every aspect of our interconnected world. As we navigate the ever-evolving landscape of cybercrime, it is imperative for the internal audit profession to grasp the magnitude of this challenge, and proactively adapt to protect our organizations and stakeholders.

The World Economic Forum warns that current cybersecurity measures are becoming obsolete in the face of increasingly sophisticated cybercriminals. According to Cybersecurity Ventures' 2022 Official Cybercrime Report, the staggering cost of cybercrime, predicted to reach \$8 trillion this year and projected to soar to \$10.5 trillion by 2025, is a grim reminder of the urgency to act.

In conversations with auditors around the world, cybersecurity is consistently mentioned as a — if not the — top concern. This challenge impacts everyone.

There's no shortage of alarming statistics to highlight the importance of this issue. A report from Juniper Research predicts that, just this year, cybercriminals will steal 33 billion records. The human element remains the most common threat vector, with human error responsible for a staggering 82% of data breaches, as revealed by Verizon's 2022 Data Breach Investigations Report. The Cybersecurity Ventures report predicts that by 2031 ransomware will cost the global economy \$265 billion annually.

And as business becomes more technology-reliant, the opportunities for cybercrime grow. Increasing adoption of cryptocurrency means a rise in crypto crime, which the Cybersecurity Ventures report says will cost the world \$30 billion annually

by 2025. Finally, the workforce gap in the cybersecurity profession, a shortfall of 3.4 million jobs globally, according to the 2022 (ISC)² Cybersecurity Workforce Study, exacerbates the challenge.

As internal auditors, we must equip ourselves with the knowledge, skills, and resources to stay ahead of cybercriminals. We must foster organizational cultures of cybersecurity awareness and provide ongoing education to our stakeholders to help them identify and respond to threats. Collaboration, both within and across organizations, is essential to staying ahead of emerging cyber risks.

Furthermore, internal audit must work hand in hand with technology experts, policymakers, and regulators to shape robust cybersecurity frameworks that ensure privacy, security, and resilience. The IIA is actively engaging in discussions with these parties to contribute our expertise and drive the necessary changes to safeguard our members, stakeholders, and the broader digital ecosystem.

Cybersecurity demands unwavering commitment and collective action, and we must confront this reality head-on. The internal audit profession must take a leadership role in fortifying our organizations' defenses and ensuring they are capable of withstanding more sophisticated and relentless cyberthreats. Together, we can secure a future where organizations thrive in a digitally enabled world.

Anthony Pugliese

internal auditor

August 2023

Published by



The Institute of
Internal Auditors

IIA President and CEO

Anthony Pugliese, CIA, CPA, CGMA, CITP

IIA Chairman of the Board

Sally-Anne Pitt, CIA, CGAP

Social Media

 @TheInstituteOfInternalAuditors

 @TheInstituteOfInternalAuditorsInc.

 @theiia

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

Editorial Advisory Board

Dennis Applegate, CIA, CPA, CMA, CFE

Lal Balkaran, CIA, FCPA, FCGA, FCMA

Robin Altia Brown

Adil Buhariwalla, CIA, CRMA, CFE, FCA

Wade Cassels, CIA, CCSA, CRMA, CFE

James Fox, CIA, CFE

Nancy Haig, CIA, CFE, CCSA, CRMA

Sonja Heath, CIA

J. Michael Jacka, CIA, CPCU, CFE, CPA

Sandra Kasahara, CIA, CPA

Michael Levy, CIA, CRMA, CISA, CISSP

Merek Lipson, CIA

Michael Marinaccio, CIA

Joe Martins, CIA, CRMA

Rick Neisser, CIA, CISA, CLU, CPCU

Manish Pathak, CA

Bryant Richards, CIA, CRMA

James Roth, PHD, CIA, CCSA, CRMA

Jason Stepnoski, CIA, CPA, CFE, CISA

Jerry Strawser, PHD, CPA

Glenn Sumners, PHD, CIA, CPA, CRMA

Robert Taft, CIA, CCSA, CRMA

Brandon Tanous, CIA, CGAP, CRMA

Robert Venczel, CIA, CRMA, CISA

Eng Wan Ng, CIA, FCPA, CGMA, ACMA

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. Copyright © 2023 The Institute of Internal Auditors Inc. Change of email address notices and subscriptions should be directed to IIA Customer Relations, +1-407-937-1111.

Opinions expressed in *Internal Auditor* may differ from policies and official statements of The Institute of Internal Auditors and its committees and from opinions endorsed by authors' employers or the editor of this journal. *Internal Auditor* does not attest to the originality of authors' content.

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



editor's note

Passing the Test

Imagine you receive a video call from your company's CEO asking you to transfer funds for an important initiative. You recognize the executive's face and voice on camera. How would you respond?

What if you are the CEO and you receive a call from a long-time supplier, demanding payment to a new account? Would you authorize the transaction? What if it isn't real? That recently happened to the CEO of a U.K. energy company who was fooled by an artificial intelligence (AI)-based call into transferring funds to what he thought was a legitimate supplier. Phishing in the age of AI and deepfakes is a far cry from what you encounter in your company's annual cybersecurity training.

AI has made a quantum leap in the past year, putting advances like generative AI in the hands of everyone — even the bad guys. That has set AI on a collision course with one of the top risks organizations face — cybersecurity. Is your organization ready for that threat?

Cyber threats are like an invasive weed running amok across the landscape. Just when organizations think they are getting them under control, something new comes along — something worse. Their roots burrow deep into an organization's networks and systems, so deep cybersecurity teams may not know they are there. It's a constant fight to mitigate these risks before they can do irrevocable damage.

In the August issue's cover story, Neil Hodge explores the many ways AI-related cyber and privacy risks are becoming "A Growing Threat" (page 34), from systems making unethical predictions, to privacy law violations, to deepfake-driven phishing attacks. "Organizations may not be aware of the specific cybersecurity and privacy risks associated with AI, or they may not understand how AI systems work and how they can be vulnerable to attacks," says Darron Sun, head of IT at Hong Kong Housing Society.

Next in "Hidden Depths" on page 41, James Bone details how organizations may lack the data on cyber risks to fully understand the impact and vulnerabilities that can lead to data breaches and compromised systems. Addressing today's threats takes a strategy that treats cyber risk as a business risk by focusing on the processes and activities that rely on technology, writes Daryl Pereira in "Mobilizing a Cyber Risk Strategy" on page 47. Pereira describes the steps internal auditors should take to audit their organization's cybersecurity strategy.

As cyber risks evolve, internal audit must be vigilant and work with the board, management, and cybersecurity experts to understand, identify, and protect against the latest threats. With AI escalating risks, auditors and their organizations can't afford to fail this test.

TimMcCollum10

Connect Risk. Connect Your Teams.

TOP-RATED AUDIT SOFTWARE ON



▶ REQUEST A DEMO AT [AUDITBOARD.COM/DEMO](https://auditboard.com/demo)



update

Data Skills Deficit

Many CAEs find it hard to fill tech roles, but some are realizing success with existing employees.

In a new report from The IIA and Grant Thornton, 85% of CAEs report that incorporating automation and analytics adds value to their internal audit functions. Yet 60% say it is difficult or very difficult to hire staff with data analytics skills.

According to “Increase Your Data Analytics ROI,” not having enough data analytics talent on staff is a key inhibitor to using data analytics for 35% of CAEs. Other challenges to successfully launching an analytics program include poor data access or quality (42%) and an inability to set up continuous data connections (34%).

CAEs who report success in finding employees with data analytics skills say their organization’s culture, opportunities, competitive compensation, and remote work options have the greatest effect on hiring and retention.

Meanwhile, many internal audit leaders are providing data analytics training to existing employees or partnering with internal or external analytics experts to successfully use analytics. In fact, 59% of respondents say assigning data analytics tasks to staff was easy or very easy, while 38% say it was easy or very easy to train current staff.

For internal audit leaders with analytics programs, 67% report using the tools to evaluate internal controls. Slightly less-common applications include employing data analytics for trend analysis, data visualization, and fraud detection. When asked where data analytics adds the most value, CAEs’ top responses were internal controls (44%), fraud detection (39%), and Sarbanes-Oxley compliance (30%). —**Logan Wamsley**

AN ACTION-PACKED YEAR

55%

THE U.S. SEC’S LATEST YEAR-OVER-YEAR

INCREASE in enforcement actions to deter accounting fraud and audit failures.

SOURCE: CORNERSTONE RESEARCH, SEC ACCOUNTING AND AUDITING ENFORCEMENT ACTIVITY YEAR IN REVIEW: FY 2022



Untapped Potential

Disengaged employees represent an opportunity for organizations.

Globally, engagement at work has bounced back to pre-pandemic levels, with 23% of the world’s workers reportedly thriving and

engaged at work, according to Gallup’s 2023 State of the Global Workplace Report. Much of the rebound in engagement comes from

workers in South Asia, which includes India.

Gallup’s annual report, which also measures employee stress and anger, offers a mix of good and bad news for employers. While South Asia pushed the U.S. and Canada out of the top spot for engagement and ranks lower for stress, the region is also home to some of the world’s angriest employees. And employees in East Asia — particularly younger workers and remote workers — tied with employees in the U.S. and Canada as the world’s most stressed wage earners. Meanwhile, Europe ranks low for stress

and anger, yet employees there report the lowest levels of engagement worldwide.

Gallup defines engaged employees as ones who find pride and meaning in their work and feel connected to their team and organization. While 18% of workers are “actively disengaged,” most workers fall somewhere in the middle, with 59% defined simply as “not engaged.”

“The world is full of untapped potential,” says Pa M. K. Sinyan, a managing partner at Gallup, “with six in 10 of us not necessarily going the extra mile, not feeling driven to achieve more than we could.”

Gallup estimates the cost of low engagement to the global economy is \$8.8 trillion, or 9% of global GDP. “When we’re engaged, we take ownership. When we see something wrong, we speak up,” Sinyan says. “It means mistakes that could happen down the line are pre-empted or prevented.”

Improving culture and managing employee stress is positively correlated to engagement, according to the study. Only 30% of engaged workers experience daily stress compared with 56% of actively disengaged workers. —Christine Janesko

FIVE

THINGS TO KNOW About the ISSB Disclosure Standards

According to the International Sustainability Standards Board, IFRS S1 and IFRS S2:

1

Provide a single, global baseline for sustainability disclosures.

2

Are designed to reduce duplicative reporting.

3

Help companies cost effectively communicate worldwide.

4

Are designed to be provided alongside financial statements.

5

Are interoperable with Global Reporting Initiative standards.

SOURCE: INTERNATIONAL FINANCIAL REPORTING STANDARDS, “TEN THINGS TO KNOW ABOUT THE FIRST ISSB STANDARDS” (JUNE 27, 2023)

ASK AN EXPERT

A Culture of Innovation



Teri Petree, CIA, PMP, is a senior director in Audit & Assurance at GSK in North Carolina.

What kind of culture promotes innovation?

Culture is one of the most important elements of an environment that promotes innovation and a passion for discovery. Important drivers of innovation are clear objectives, recognition, and accountability.

Setting the right objectives is central to any leader's strategy. The old adage that "what gets measured gets managed" rings true in organizations struggling

to break down negative headwinds. Setting objectives that encourage ownership and partnership will support a desirable culture.

Recognizing positive traits in individuals and teams also creates a positive culture. People need to feel engaged in their work in a way that draws them in and promotes creative innovation. Freedom to fail means rewarding people for taking chances, regardless of the outcome, if done with appropriate governance and controls.

Accountability starts with giving people defined boundaries so they understand where they can safely operate, which leads to confidence. A lack of clear boundaries creates fear — the enemy of innovation.

How can internal audit support a culture of innovation?

An auditor's primary goal should be to inspire, not enforce, meaningful action. Responding to findings is not optional, but the approach and style of the audit team can dramatically influence the reception and value of each engagement.

A risk management culture should be understood as proactively managing

risk while increasing efficiency and effectiveness in innovative areas such as research and development. Findings should be seen as opportunities to improve, while corrective and preventive action plans enhance the company's ability to diagnose, evaluate, and deliver its best solutions.

The audit function is there to help preserve the future and prime the organization for success.

Accountability starts with giving people defined boundaries so they understand where they can safely operate, which leads to confidence. A lack of clear boundaries creates fear — the enemy of innovation.

Risky Health Delays

58%

of employees delay necessary medical care due to cost or insurance barriers.

42%

report delays because there isn't an appointment available.

55%

of employees in rural areas are up to date on preventive screenings, compared to 61% in urban areas.

SOURCE: INTEGRATED BENEFITS INSTITUTE, 58% OF EMPLOYEES DELAYED NECESSARY MEDICAL CARE DUE TO COST OR INSURANCE BARRIERS



Thank you

to everyone who commented on the proposed *Global Internal Audit Standards™* during the public comment period. The International Internal Audit Standards Board is analyzing the comments received as it works to finalize the *Standards™* before the end of the year.

Have questions?

Learn more at theiia.org/IPPFevolution.



The Institute of
Internal Auditors

basics

Digging into DEI

Internal auditors need insight into what diversity, equity, and inclusion look like in practice.

◆ Wade Cassels

Diversity, equity, and inclusion (DEI) are key success factors for all organizations, and as such, they should be squarely in the sights of internal audit. However, because these traits are not

easily quantified, some auditors or internal audit teams may feel uncertain about how to provide assurance around them. Having clear working definitions of what these terms mean and what they look like in practice is crucial to providing assurance with confidence.

Defining the Terms

Organizations cannot have meaningful conversations about DEI if their people are not all talking about the same thing. A shared understanding of the meaning of DEI is critical to any effort to assess or improve in this area. As internal audit works across departmental lines, it is important for auditors to get a sense of whether employees' understanding of what these terms mean is accurate and aligned. As such, a review of company training materials would be a good place to start a DEI-related audit.

Diversity is best thought of simply as variety. It means having people in the organization who collectively represent a broad range of characteristics. Diversity applies to people's biology, such as sex, race, ethnicity, skin color, disabilities, and age, as well as their nationality, language, and culture. Organizations should be intentional in exhibiting variety across these characteristics. Mature organizations look beyond these characteristics.

Companies genuinely committed to diversity comprise people with different backgrounds and experiences, too. Their resumes will include work experience in a variety

of industries, companies, and countries. Some will have backgrounds in the military or other public service; others will not. Some will have advanced college degrees; others will not. And so on.

Each person's cumulative work and life experience add to the diversity of the organization by contributing unique thoughts, attitudes, and perspectives that benefit organizations through better decision-making, stronger engagement with the communities they serve, and a more inclusive culture.

Equity means fairness and impartiality. Organizations should embody equity's fairness when dealing with the treatment of employees and the extent to which they are given an equal opportunity to maximize their own potential.

Sometimes equity means treating everyone the same, but it doesn't always mean that. It is fair for the president of the company to earn more than an entry-level analyst. The spirit of equity has more to do with ensuring that preferential treatment is not unfairly reserved for certain people (i.e., favoritism), or conversely, that barriers or constraints are not placed unfairly on certain groups or individuals.

For auditors, key areas to look at regarding equity are job openings and promotions, benefits, perks, pay, and information. If all employees in a company believe they receive fair and justifiable access to these things, there is a good chance the organization is fulfilling its commitment to equity.

Ensuring a fair and equal opportunity hiring process from candidate selection to onboarding is foundational to building a diverse, inclusive organization. Conducting a discreet risk assessment around the hiring process to identify unfair practices or potential biases should be within the scope of any audit function looking at DEI. However, organizations

can do more than just look to eliminate inequities.

Mature organizations reach out proactively to underrepresented groups and have a multifaceted talent pipeline that provides equitable access for people of different cultures, locations, and socioeconomic groups to apply for open positions.

Likewise, for internal candidates, employee growth programs such as mentoring and cross-departmental training can give employees in traditionally underrepresented groups the chance to be seen. When internal hires are made, this opportunity will ensure the candidate pool includes a more diverse group of “known” prospects.

A mature approach to DEI also considers interactions with external parties, such as third-party suppliers and business partners, distribution channels, media, and communities.

Inclusion means a culture where respect for differences across aspects such as experience, heritage, personal beliefs, and biological differences is the norm. No one is unwelcome, and everyone feels that they are a valued part of the organization.

Employees at inclusive organizations have the assurance that these personal aspects of themselves will not represent barriers to performing their duties or fulfilling their potential within the organization. Workers are more engaged in the organization if they believe they are welcomed and valued for the things that make them uniquely them.

Looking Inward and Outward

Naturally, organizations (and their auditors) tend to focus on the employee base when assessing their DEI. However, a mature approach to DEI also considers interactions with external parties, such as third-party suppliers and business partners, distribution channels, media, and communities. Internal auditors should ask:

- Are the third parties we deal with as committed to DEI as we are?
- Is our process for selecting vendors and partners open, fair, and equitable?

- Is our product and service assortment inclusive of different customer groups?
- If we have a target customer, are we sure our definition and understanding of our target customer is based on good information?
- Are we unintentionally excluding someone?

Perceptions of inclusiveness are tied not just to the employee base, but also to who the organization interacts with, and subsequently, that can expose the organization to risk. Internal audit should be aware of this when considering DEI on its own or within the context of third-party risk audits.

The Chief Diversity Officer

At many organizations, commitment to DEI manifests itself in the designation of a chief diversity officer (CDO). Having a CDO in place promotes accountability within the organization and ensures ownership of responsibility for DEI. Internal auditors should determine whether there is someone in the organization who is explicitly accountable for DEI.

The CDO puts a face on the organization’s DEI, and having a face is an important part of communicating



Much like the CAE, the CDO must have unencumbered access to **the board and the board's full support and authority to make unbiased recommendations.**

commitment. However, messaging is only one piece of the puzzle. The CDO also should build strategies and initiatives suited to the organization's goals and see that these strategies are carried out. Further, the CDO should stay abreast of cultural conversations and bring new ideas, trends, and concerns to the attention of others.

When there is feedback or opportunity for improvement, the CDO should ensure there is follow through. Much like the CAE, the CDO must have unencumbered access to the board and the board's full support and authority to make unbiased recommendations.

Timeless Concepts

DEI comprises timeless concepts that are easy to grasp. Nevertheless, circumstances in the marketplace and the world change over time, present new challenges, and require fresh approaches. Success is fostered by candid conversations and open communication.

From an auditor's point of view, the core of the test boils down to genuine top-down commitment, shared definitions/understanding, accountability for actions, and built-in mechanisms to ensure meaningful conversations continue to take place.

Wade Cassels, CIA, CISA, CFE, is senior auditor at Nielsen in Lakeland, Fla.

INTRODUCING The IIA Resource Hub

Our library of free downloadable content includes white papers, webinars, product guides, case studies, industry analysis and much more.

TheIIAHub.org



Govern, Protect & Audit Data

Data Privacy Assurance Forum

OCT. 12, 2023 • EARN 6.6 CPES

Register Today



tech

Control in the Cloud

Internal audit can review key controls to help ensure operations are both secure and well-managed.

◆ Michael Ratemo

Research firm Gartner predicts that 99% of cloud security failures through 2025 will be caused by a cloud customer error. That is because many of the businesses that have flocked to the cloud are not familiar with processes and controls for securing it. As a result, a

security oversight can easily expose an organization's cloud-based resources to attackers.

Despite its many benefits, the cloud also presents unique security risks and challenges. When a company owns and manages all parts of its IT infrastructure, it has complete control over its data. However, in the cloud, organizations store their data

with a third-party provider, limiting visibility and control over that data.

Organizations not only need to ensure their data is secure, they also must make sure cloud operations are well-managed and costs are controlled. Internal auditors can help by reviewing the key controls that are critical to cloud operations, focusing on six areas.

Realize Shared Responsibility

The cloud operates on a shared responsibility model, which describes what the cloud customer and cloud service provider are each responsible for. It's essential for cloud customers to understand their responsibilities.

The cloud customers should ensure services are implemented securely. For example, IT should add the cloud service to its existing inventory to verify it is managed according to organizational policy. Likewise, information security should assess whether the cloud providers' controls are adequate for the type of data the organization will be storing.

The level of responsibility depends on the deployment model (public, private, community, or hybrid) and service type. As an organization moves from software as a service (SaaS) to platform as a service (PaaS) to infrastructure as a service (IaaS), its responsibility grows — and so does its risk. For example, SaaS customers are not responsible for applying security patches to applications, but IaaS customers are responsible for patching any application installed on the infrastructure. Internal auditors should ensure the organization understands its obligations and has defined roles and responsibilities.



Manage Shadow IT

Because cloud environments can be accessed directly from the internet, users can easily bypass the organization's procurement processes to choose the cloud solutions they want. For instance, users can deploy a server in the cloud without the organization's knowledge. This is called shadow IT. The risk with shadow IT is it places corporate data outside the protection of the organization's security controls, increasing the risk of a data breach.

Internal auditors should evaluate whether the organization leverages tools to track which cloud services are being accessed. This helps ensure employees are not using unauthorized and unsupported cloud services.



Monitor Resource Usage and Costs

The biggest cloud service providers offer hundreds of services. Yet having so many options leads many cloud customers to choose the wrong services because they plan poorly and do not understand the business's requirements. Often, these services go unused, wasting money.

Moreover, cloud service providers have complex pricing models, with rates that change according to service, region, and other parameters. An organization may incur unexpected costs if it does not fully understand a cloud service provider's pricing model or how the pricing varies per usage.

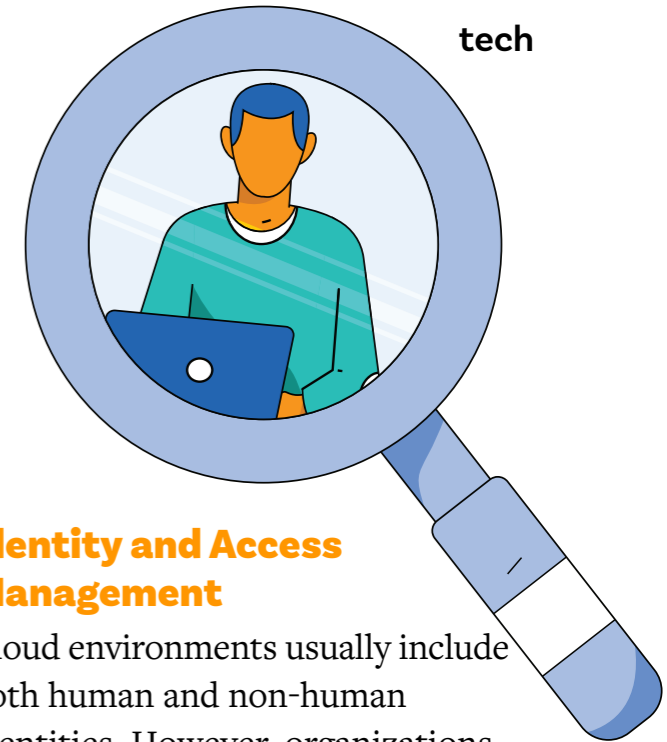
Internal auditors should determine whether the organization is using cloud cost management tools for tracking cloud usage and associated costs. In addition, auditors should evaluate whether the organization inventories resources in the cloud using a process called tagging. Tagging applies metadata to help describe and identify the resources running across an organization's cloud environments. Tagging is essential for gaining visibility into an organization's cloud consumption and expenditure.

Secure Cloud Configuration

Because cloud technology is still an emerging market, many organizations are unaccustomed to securing cloud infrastructure. Secure cloud configuration refers to adjusting the default settings of a cloud system to mitigate security risk. If the cloud system settings are not tuned appropriately, this could result in cloud misconfiguration — one of the top cloud security risks that attackers look to exploit.

An example of a cloud misconfiguration is mistakenly making a cloud-based data repository publicly accessible when it was meant to be private — opening the repository to anyone on the internet. Attackers use tools designed to search the internet for these unsecured cloud deployments.

To address cloud misconfiguration, internal auditors should determine whether the organization scans and reviews its cloud workloads for common vulnerabilities, such as exposed access points and resources labeled as public. Organizations can perform these scans using cloud security posture management tools that identify misconfiguration issues and compliance risks.



Identity and Access Management

Cloud environments usually include both human and non-human identities. However, organizations often create these environments with overly broad permissions that allow unregulated access to cloud resources. Attackers who have gained initial entry into a cloud environment can leverage these broad permissions to escalate access and move laterally inside the cloud infrastructure.

Organizations should implement strong identity access management practices to oversee digital identities and control user access to an organization's data. Other ways to minimize access risks include:

- Using role-based access control and the least privilege principle.
- Enabling multifactor authentication of users.
- Performing regular reviews of all identity roles and policies.

Shop the Latest Releases & Stock Up on Knowledge

IIA members enjoy 20% savings on publications every day.



**BOOK
OF THE MONTH
Savings**

The Internal Auditor's Guide to Risk Assessment, 2nd Edition

SAVE AN EXTRA \$10*

With Promo Code 2023IAG10

*Valid through August 31, 2023



Shop now.
theiia.org/bookstore

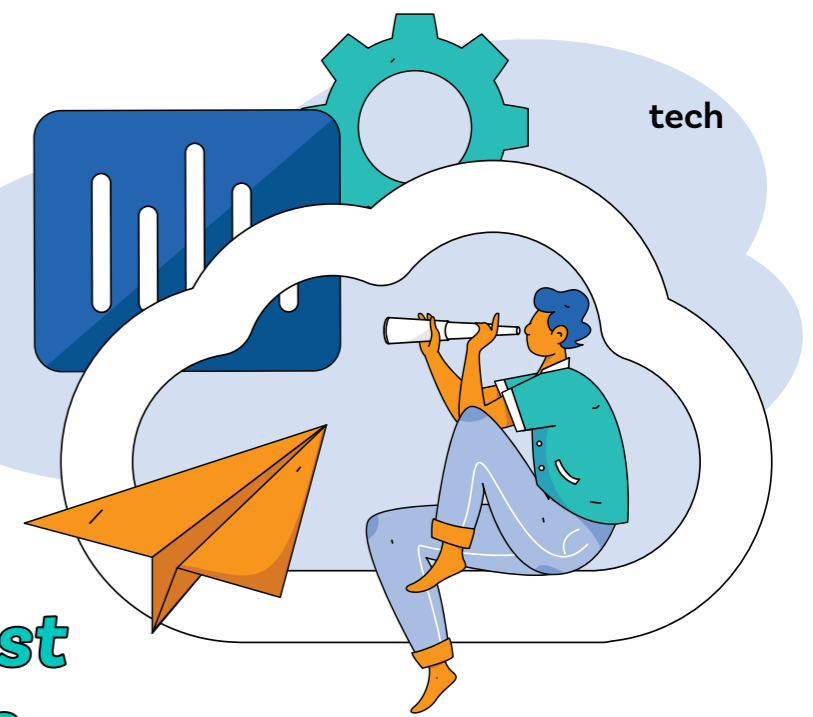


Automating routine security tasks will mitigate most manual risks presented by human error.

Automate Routine Tasks

Many organizations execute processes in the cloud manually, including installation and configuration of virtual servers, networks, storage volumes, and other cloud resources. These manual processes are time-consuming, error-prone, and hard to scale. Automating routine security tasks will mitigate most manual risks presented by human error.

Internal auditors should examine the organization's use of automation within its cloud environments. One way an organization can implement cloud automation is by using



infrastructure as code, which is a process of creating cloud infrastructure through templates defined by code. Once developed, infrastructure as code provides reusable templates for creating virtual machines, storage, networks, and other infrastructure components.

Optimize the Cloud

As organizations increasingly move to the cloud, internal auditors need to be prepared with the tools and knowledge to assess the risks. These capabilities will enable auditors to provide tailored recommendations that help mitigate risks and allow the organization to leverage the cloud in an optimum manner.

Michael Ratemo, CIA, CISA, CISSP, CCSK, is principal consultant at Cyber Security Simplified in Austin, Texas.

Cybersecurity plays a critical role in the environmental, social, and governance sphere.

THE C IN ESG

It has become abundantly clear over the past few years that the breadth of topics that fall under the environmental, social, and governance umbrella is expansive. Here are just a few of the many areas that are included under each ESG pillar:

Environmental (E). The myriad of topics included under the “E” pillar include climate change (generally viewed as

global warming), water use and accessibility to clean water, waste and pollution reduction, land use and biodiversity, and resource depletion.

Social (S). The “S” in ESG is generally defined as an organization’s operational impact on society and how organizations are promoting social diversity and inclusion with a focus on diversity, equity, and inclusion;

employee well-being; and community engagement.

Governance (G). The “G” encompasses factors such as board and management composition, corporate structure, business ethics, and anti-corruption. This includes company policies, standards, information disclosures, and audit and compliance issues.

A topic that seems to be flying below the ESG radar for

many organizations, yet should be a top consideration, is cybersecurity. Organizations battle many cyber-related threats that tie directly back to ESG, including data breaches, ransomware attacks, and more. Failure to manage those threats effectively can create exposures to the organization such as the loss of critical assets ranging from employees’ personal information

to customers’ and other stakeholders’ private information.

These types of cyber incidents are typically viewed within the social and governance pillars of ESG, and they can lead to customers, employees, and third parties losing trust in an organization. Ultimately, this can cause significant harm to the organization’s reputation and financial stability.

With websites becoming more sophisticated at capturing user data along with the emergence of artificial intelligence, machine learning, and robotic process automation, the stakes are rising for cybersecurity teams as they battle to protect data assets of all types.

CYBERSECURITY COLLABORATION

With evolving ESG regulations and new cybersecurity threats emerging at a relentless pace, internal auditors have an opportunity to add value by working closely with the cybersecurity team to proactively identify emerging threats and implement mitigation strategies.

Internal auditors should keep in mind a few key considerations as they venture into what may be unfamiliar territory:

Offer a strategic perspective. Internal audit should work to address cyber threats consistently across the organization and avoid siloed approaches. It should collaborate with other teams that might have relevant information or perspectives.

Maintain independence.

While internal audit does focus on providing assurance services, advisory services are allowable and even encouraged, but auditors should be mindful not to take on the role of management by making decisions or “doing the work.”

Be nimble. The rapid evolution of cybersecurity threats

means an agile approach is crucial. This will enable internal audit to provide insights while they are still relevant.

Provide coordinated and consistent risk information.

Internal audit should share timely risk information with management and the board to enable quick and decisive action. Internal audit needs to

provide its independent assessments; however, by working with the cybersecurity team, it can avoid confusing or conflicting information that undermines board and management confidence in the function.

With cybersecurity being a key element of an organization's governance structure as well as

being foundational for an effective data privacy program, now is the time for internal audit teams to secure a seat at the table. By ensuring cybersecurity threats are reflected in the organization's ESG program and continuously working to understand and mitigate those threats, internal audit can help protect the organization and maximize its impact.

ENGAGING WITH CYBERSECURITY ALLIES

Building strong relationships is nothing new for internal auditors, but the importance of collaboration across teams when it comes to cybersecurity cannot be understated. Auditors need to work closely with all parties involved, especially their organization's chief information security officer.

The IIA provides guidance on getting started developing those critical relationships:

GTAG: AUDITING CYBERSECURITY OPERATIONS — PREVENTION AND DETECTION provides guidance on how internal auditors can examine and prioritize assurance over cybersecurity operations. It aims to help internal auditors understand and audit cybersecurity operations across their organizations.

GLOBAL KNOWLEDGE BRIEF: CYBERSECURITY IN 2022, PART 2, CRITICAL PARTNERS — INTERNAL AUDIT AND THE CISO addresses the importance of developing a strong relationship with the CISO. It makes a case for creating a healthy relationship for effective assurance that doesn't jeopardize internal audit's independence.



risk

Lending a Hand

Employee loan programs offer both risk and reward for employers.

◆ David Dominguez



Organizations around the globe provide loans to their labor force for a variety of reasons. Some are required to offer loans to comply with collective agreements or specific local labor laws and regulations. Other entities willingly offer employee loans to differentiate themselves in talent acquisition or retention efforts. Offering loans may help organizations attract job candidates, boost employee loyalty and morale, and reduce turnover.

Regardless of the circumstances, an employer-employee loan is a delicate matter that must be appropriately managed. While employee loan receivables are not usually materially significant to an organization's finances, employee loans should be on internal audit's radar, given that their inadequate or inconsistent treatment can introduce risks that have repercussions both for the company and the employees.

A Mixed Bag

Although employee loan programs are not new, current financial constraints are prompting more employees to turn to their employers to request a loan in lieu of, or as a complement to, obtaining financing from traditional lending

institutions. Increases in employee turnover, inflation, and interest rates, along with the need to look more generous than competitors, are prompting companies to reconsider their compensation and benefits packages.

Multinational organizations often have multiple loan programs, with each tailored to the needs and requirements at the specific location. International entities are subject to a variety of employment practices, labor law requirements, and even labor unions that may include loans as part of their bargaining negotiations.

Some employers are required to have a range of special purpose loans. In addition to generic loans, for example, companies may offer loans to cover unexpected medical expenses or to assist in purchasing a home.

In certain countries, employers are required to conduct credit checks on all loans, while others have such requirements only when loans are over a specific amount. Countries, including the U.K. and South Africa, require employers to register or file reports with a specific government agency. The mere fact that the employer grants a loan to an employee triggers a set of requirements and periodic regulatory reporting to the government. In other cases, employers must carefully

keep track of payroll deductions, as regulations limit monthly and annual aggregate amounts deducted.

In companies that operate in one country, requirements may vary by state or province. Most states allow companies to deduct loan installment payments through automated payroll deductions if the employee's wages do not fall below federal minimum wage. Most require that employees agree to these deductions in writing. Some states, like California, specifically prevent employers from recovering most unpaid loan amounts via lump sum deductions from former employees.

These country-by-country and even state-by-state differences complicate the employer's ability to grant, manage, and collect employee loans.

Assessing the Risks

When it comes to employee loans, internal auditors can provide assurance or advisory services in several areas.

Governance. There should be written policies and procedures for loan programs. The program should have clearly defined terms delineating circumstances under which a loan will be provided, as well as details on key items such as:

- Minimum and maximum loan amounts.

- Loan durations.
- Interest rates.
- Installment payments.
- Early repayment options.
- Number of loans outstanding.
- Recourse and credit checks.

In some instances, an internal committee is formed to review and decide on loan applications and to monitor the loan program.

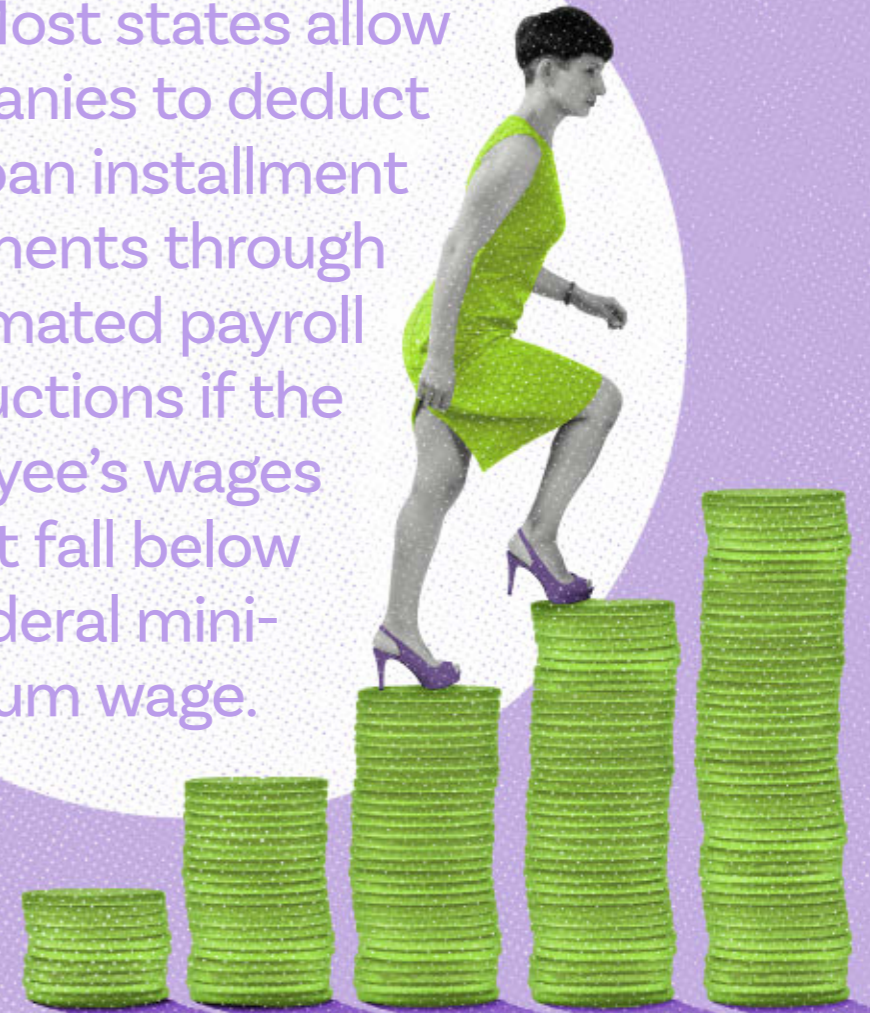
Record management. Similar to other company records, organizations need discipline around their records management on all loan applications and supporting documentation, decisions to grant or deny loans, and executing agreements for each loan granted with clearly defined terms.

Taxes. There are many tax implications for the employer and employees and, in some cases, former employees. Complications are triggered by matters such as interest rates (e.g., providing loans without specifying the rate or at below market rates) or potential forgiveness of balances.

Accounting and finance. Accounting items to address include correct recording, disclosing, and reconciling measures. Areas to consider include:

- Correct accounting and classification for loans over one year as compared to those one year or less.

Most states allow companies to deduct loan installment payments through automated payroll deductions if the employee's wages do not fall below federal minimum wage.



- Controls around granting, funding, and collection activity.
 - Approvals for financial losses resulting from various events, including instances where employees leave their jobs and the entity is limited or prohibited in its efforts to collect loan balances. This may require companies to write off such loans.
 - Mechanisms to prevent commingling of bank accounts used for granting and collecting loans with other accounts that the organization may have. Or, if applicable, commingling of multiple loans with various terms granted to the same employee.
- Payroll.** Organizations should have processes and procedures for

Let's be Frank

“By failing to prepare, you are preparing to fail.”

September 11-12, 2023

The Financial Services Exchange is prepared to tackle the toughest topics – from risk to regulatory reform and cybersecurity to cryptocurrency. Whether your audit or examination focus is on banking, insurance, money-management, crypto, NFTs, or other financial service topics, this year's event will help you find your failsafe.

Washington, DC • theiia.org/FSE



risk

collecting the right amounts with the correct periodicity and ensure these follow any minimum or maximum regulatory monetary thresholds.

Fraud. Employee loans may be vulnerable to fraud. Segregation of duties around loan approval, funding, recording, reconciling, collection, and write-offs must be in place to detect and prevent abuses or irregularities.

Regulations. Certain statutes prohibit companies from providing loans to specific individuals. In the U.S., publicly traded companies are not allowed to give loans to directors and officers. It also is imperative to consider related-party transactions. Discrimination risks can arise if it is not clear why loans are provided to certain employees but not others.

Administration. Loan programs require time and effort to maintain and manage. There may be opportunities to automate certain tasks or processes in the overall employee loan cycle.

Weighing the Options

Some companies choose not to provide loans or point employees to other options such as loans under

Discrimination risks can arise if it is not clear why loans are provided to certain employees but not others.



company or government-sponsored retirement plans. However, offering loans can demonstrate a focus on socially responsible initiatives.

Companies must be aware of the risks employee loans present. Internal auditors need to focus on the right risks to strategically audit or review the governance, risk management, and controls over this area.

David Dominguez, CIA, CRMA, CPA, CFE, is the director of audit and compliance at a publicly traded company in Houston.

fraud

Accessories to Theft

A clothing store clerk and her friends fashion fictitious returns for extra cash.

◆ Laura Harris ◆ Joshua Clark

Casey's Corner has long been a popular clothing store in the historic town of Taylorsburg, Ohio.

The store was named after the owner's daughter, Casey Burn, who now runs the operation. Like her mother, Burn was proud of the store's sophisticated cocktail of modern, distinct style; unbeatable customer service; and old-fashioned charm.

Burn hired students from local high schools and nearby colleges as retail clerks to keep the atmosphere fun and fresh. One of the clerks was Tara Jay, a friend's daughter who was home from college for the summer and taking the year off to earn

money for school. It wasn't long before Jay came up with a wonderful idea to draw in more customers that Burn loved: Every other week, when the new product shipments came in, the store would hold social events such as tea parties, girls' nights, and cookie club.

Burn was in the process of opening another store and sales seemed better than ever. Because she was so busy, she asked her friend Sam Knox, an internal auditor at a local bank, to help by checking the store's accounts a few times each quarter. During one of her checks, Knox noticed a strange pattern emerging. Sales were high, but the revenue didn't seem to be flourishing.



Knox considered why a slump might be possible. Summer was a good time for the store as many of the college-aged customers were home. When fall came, sales would slow down, but the parties Jay had arranged should have kept the locals involved. How could Casey's Corner be selling more but earning less?

A closer look at sales information from the previous six months turned up a disturbing trend — lots of customers appeared to be returning merchandise. Each return resulted in refunds between \$100 and \$200, yet there was never a corresponding sales record.

Knox looked through the returns until she spotted a name she recognized. On a hunch, she gave Muriel Fond a call. Knox explained that she was helping Burn go through her

accounts. "I see you returned some things recently," she said. "Did they not work out for you?" But Fond said she hadn't returned anything. Indeed, she said she loved the store and enjoyed bringing her granddaughters in for shopping.

Knox next examined the rest of the credit accounts. Some customer accounts showed no recent purchases but had received returns for merchandise purchased months earlier. Newer customer accounts showed purchases and returns on the same credit card every month.

The refunds were not individually significant, but they quickly added up to an amount that made Knox raise an eyebrow. Even more disturbing — the purchases were on credit cards, but many of the refunds were in cash. If the recent

activity on Muriel's account was any indication, Knox suspected the rest of these accounts had also not returned any merchandise.

Then there was the question of inventory. On the books, inventory looked full, but Burn had just mentioned how fast the new line of purses was selling and how the store would need to order more.

By looking at the store's sales data, calculating its inventory turnover, and examining returns and voids, Knox surmised what was happening. She told Burn what she suspected; someone was being unfashionably generous with refunds. The two decided to attend the next store event and keep a close watch on what was sold to whom, and by whom.

Knox knew the fraudster had to be one of the cashiers, as they had

the ability to conduct returns. At the next store event, she noticed that one cashier was very active behind the register. Knox reconciled the receipts from the night of the party and for a few days after.

The returns only occurred on the days in which Jay worked. It seemed the college student had found a way to make more than a little extra money, after all.

Burn and Knox spoke with Jay's co-workers and learned that many of Jay's friends would come in and insist on being helped only by Jay, but they rarely bought anything.

Even though the store had no cameras to observe cashiers, Knox and Burn pieced together how Jay was stealing money. Jay would credit her friends cards each month with amounts they would later split.



On a hunch, she gave Muriel Fond a call. Knox explained that she was helping Burn go through her accounts. "I see you returned some things recently," she said. "Did they not work out for you?" But Fond said she hadn't returned anything.



2023 ESG Virtual Conference

Theory in Practice

Register by Aug. 10 & Save 10%.

It's more essential than ever to seek a greater understanding of the evolving regulatory environment, discover ways to impact the success of your organization's strategies, and use innovative techniques to improve internal controls and identify emerging risks.

Sept. 21 • 10:00 A.M. – 4:30 P.M. • EARN 6.6 CPEs
theiia.org/ESGVirtualConference



fraud

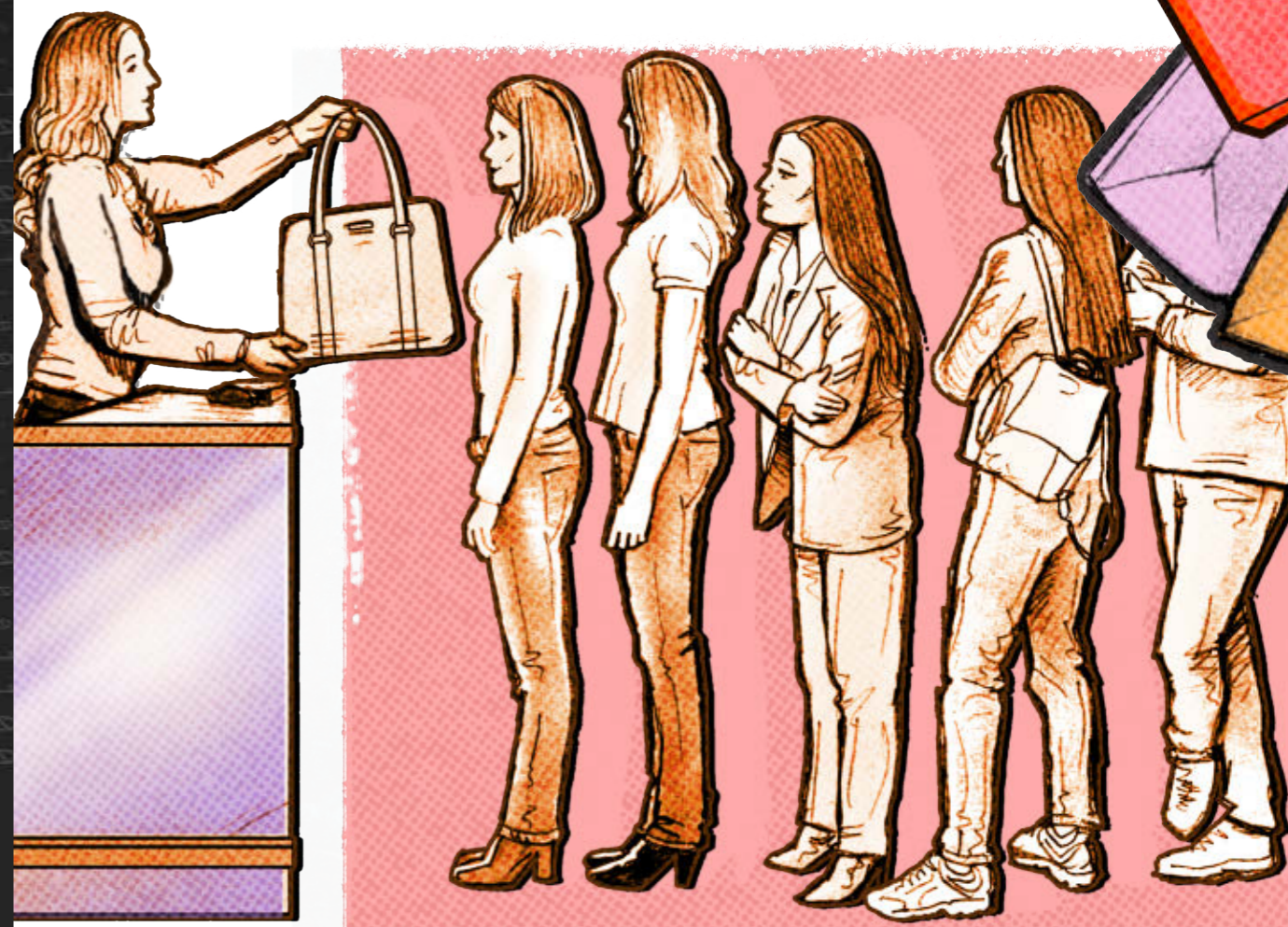
Sometimes, she would even let them keep purses and shoes that they bought, and still run a return on their cards. When that wasn't enough, she went back into older sales and conducted returns on purchases made with credit cards but kept the cash she was supposedly returning.

Jay's fictitious returns also manipulated the store's inventory. When Jay conducted a refund for an item, the store's inventory recorded one more unit in stock than what was actually available, causing the store to book a lot of invisible stock.

A serious control weakness in Casey's Corner's operations was its return policy did not require that

each refund had to be supplemented by an original store receipt. This was all Jay needed to give credits to customers for items they had never purchased. Jay's fictitious refund scheme would have been much more difficult to carry out if the store copy of every refund receipt was required to be attached to the original sales receipt.

Additionally, Jay was not required to obtain Burn's authorization to process customer credits. No other manager was available to approve or deny returns and voids. Burn wasn't diligent about reviewing the supporting documents necessary for customer credit



Jay had been running her scheme for more than six months, causing the store to lose nearly \$20,000.



transactions. She was simply too busy, and Jay knew it. Jay had been running her scheme for more than six months, causing the store to lose nearly \$20,000.

Burn fired Jay but declined to pursue charges. However, with Knox's help, Burn was able to implement

new, updated internal controls that address the fraud gap that Jay had exploited. With no further thefts, Burn was finally able to open her second venture in a nearby town.

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

Lessons Learned

Customer refunds and credits can be a place where fraud can thrive if oversight is not maintained. Management should assess all customer refund activity by their employees regularly and be aware of the frequency and size of the credits generated. Without this periodic oversight, Jay's scheme was able to continue undetected. Burn also should have reviewed all sequentially numbered refund or void transactions.

Management should be alert to customers obsessively using a particular salesperson. Customers may have a favorite salesperson, but when a suspicious number of customers continuously refuse service by anyone other than one specific employee, this may be a warning sign to management that something devious is occurring.

Supervisors should be required to authorize customer refunds. By restricting access, codes, or the authorization required to process refunds, employees like Jay are much less able to abuse customer credit transactions individually.

Significant differences in the perpetual and physical inventory records should be investigated. Management should keep up with the changes in inventory regularly. If management discovers a difference with no sufficient explanation, it warrants a deeper analysis. Jay's scheme caused large inventory discrepancies, which, if explored, may have alerted Burn that something suspicious was occurring in her store.

Accelerate Your Success.



The IIA Congratulates the 2022 CIA Exam **Award Winners!**

As the only globally recognized internal audit certification, becoming a Certified Internal Auditor® (CIA®) is the optimum way to communicate knowledge, skills, and competencies to effectively carry out professional responsibilities for any internal audit, anywhere in the world.

Fehr Aljefri - Gold

The Saudi Institute of Internal Auditors

Joey Sacramento Jr. - Silver

IIA - Philippines

Shirley Liwen Zhang - Bronze

IIA - China

Briana Dincher - Student

IIA - Global

CRMA:

Top Winner: **Blair Wightman**

IIA - New Zealand

Visit theiia.org/TopScoreWinners for a complete list of top CIA and CRMA score winners.

Begin your journey toward the only globally recognized certification for internal auditors.

Apply today at theiia.org/CIA



The Institute of
Internal Auditors

A Growing Threat

As organizations sow AI throughout the business, they risk being overwhelmed by rampant and invasive cybersecurity and privacy threats.

◆ Neil Hodge





uch has been written about the potentially harmful impacts that artificial intelligence (AI) and machine learning can have on people

and organizations if they produce biased outcomes based on selective, incomplete, or bad data. The danger is so acute that most internal audit functions have AI high on their risk registers. Yet many organizations may be ignoring an even greater risk associated with AI use — cybersecurity and privacy.

Powerful AI-based machines can learn patterns of behavior, see and predict trends, and emulate words, actions, sounds, and pictures quicker than ever — and with tremendous accuracy. They also can deal with greater volumes of data being inputted into them. These capabilities make a variety

of risks — including fraud, ransomware, and data loss/theft — much more likely, as well as potentially ruinous.

Some companies have already been targets. In 2019, cybercriminals used a fraudulent AI-powered voice call to dupe the CEO of a U.K. energy firm into transferring €220,000 to what

“AI systems rely on large amounts of data to train models and make accurate predictions. However, this dependency on data raises concerns about data breaches, privacy, and protection.”

—**Mohammad Abdur Razzaque**, Associate Professor of Research, Centre for Digital Innovation, Teesside University



he believed was a known supplier in Hungary. In 2020, an employee at a Hong Kong company similarly fell victim to scammers using cloning technology to make the call appear to be from the CEO authorizing the cash transfers. These incidents occurred before the debut of generative AI.

Besides these scams where AI makes the request appear more believable to the victim, experts warn that the key risks organizations

must address fast are data leakage from data breaches and cyberattacks targeting machine-learning models by corrupting input data to deliberately produce incorrect predictions or decisions. Because AI algorithms usually require access to large data sets, the potential for data loss and hacking increases massively. Meanwhile, data manipulation by hackers could have catastrophic effects if people’s medical or financial

information, for example, is deliberately changed.

“AI systems rely on large amounts of data to train models and make accurate predictions,” says Mohammad Abdur Razzaque, associate professor of research, at Teesside University’s Centre for Digital Innovation in the U.K. “However, this dependency on data raises concerns about data breaches, privacy, and protection. Many organizations may not have enough knowledge and



“Even when data is anonymized, an AI algorithm may be able to de-anonymize it and re-identify an individual by correlating the data to other available data points.”

—Vera Cherepanova, CEO and Founding Partner, Studio Etica

expertise to comprehend the unique security risks associated with AI and may underestimate the importance of thoroughly testing and validating AI models and systems.”

Phishing Upgraded

Where past cyberattacks may have depended on generic phishing emails, attacks now are more sophisticated, says Will Richmond-Coggan, partner at the Oxford office of U.K. law firm Freeths and an expert in data and privacy disputes involving emerging technologies. They could involve using AI-generated emails written in the style of

the CEO or finance director with convincing instructions for money transfers or attempts to trick recipients into clicking on links to deploy payloads. The days of easily detectable phishing emails are over, he warns.

“The rapid evolution of deepfake technology means that a phishing attack might be supported with a convincing audio or even video call ostensibly from a colleague or superior within the business,” Richmond-Coggan says. “As quantum computing begins to become commercially available, much of a company’s existing security arrangements — particularly those aspects that

depend on password security and encryption — will need to be re-thought.”

Another problem auditors need to be aware of is that AI’s ability to “connect the dots” puts the need for privacy protection and data security front of mind. “Even when data is anonymized, an AI algorithm may be able to de-anonymize it and re-identify an individual by correlating the data to other available data points,” says Vera Cherepanova, CEO and founding partner at compliance consultancy Studio Etica in Bormio, Italy. That will inevitably breach privacy laws throughout the world.

Similarly, she adds, specific AI algorithms have the

potential to guess and make unethical predictions. In 2012, *The New York Times* published a story about how U.S. retailer Target had identified 25 items that when bought together indicated a customer was likely to be pregnant. The company then used that information to send women — and occasionally, children — coupons for baby products. “Today the power and accessibility of AI is far greater than it was then,” Cherepanova warns.

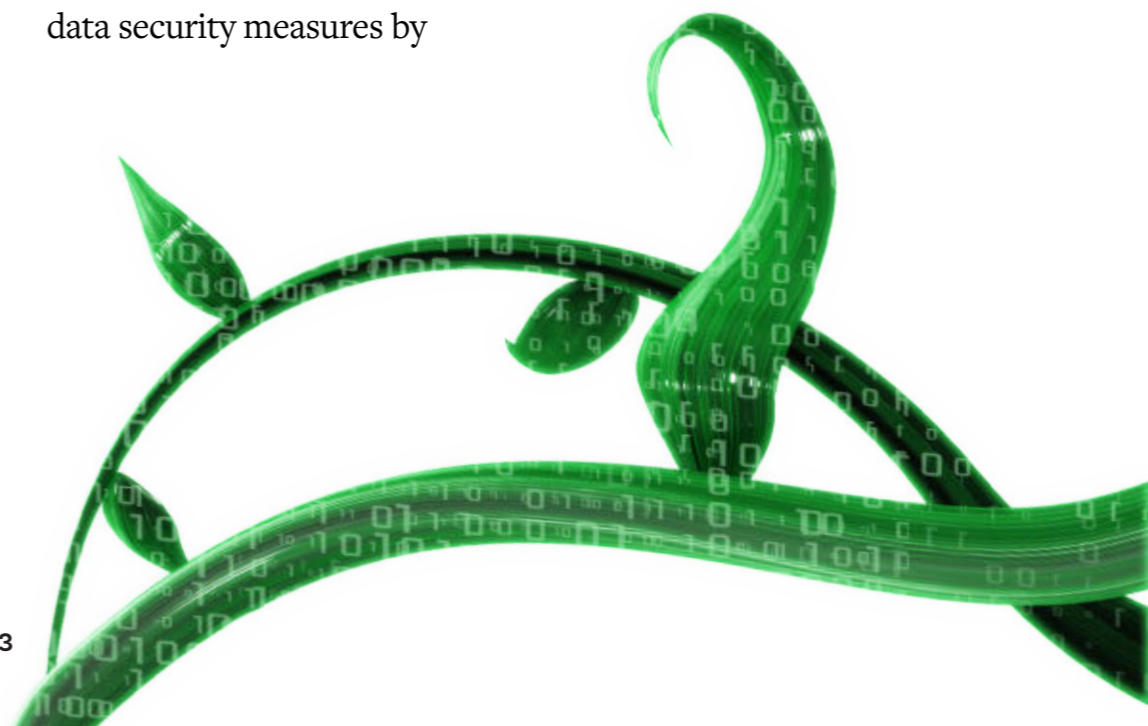
Mitigation Challenges

Organizations can take several practical steps to mitigate these risks. The most obvious, experts say, are to implement and enforce strong data security measures by

encrypting data, beefing up storage security, and limiting access to data sets.

These measures should be accompanied by regularly evaluating and updating data security protocols and policies to align with industry standards and evolving threats. Regular, proactive audits and risk assessments of AI models and their vulnerabilities are another must.

However, Darron Sun, head of IT at Hong Kong Housing Society in Hong Kong, says one of the most common mistakes in trying to mitigate AI security is failing to understand the risks associated with



AI technologies in the first place. “Organizations may not be aware of the specific cybersecurity and privacy risks associated with AI, or they may not understand how AI systems work and how they can be vulnerable to attacks,” Sun explains. “This lack of understanding can lead to inadequate risk assessments and ineffective risk mitigation strategies.”

Organizations may also fail to consider the entire AI development life cycle when identifying and mitigating cybersecurity risks, as each phase presents unique cybersecurity and privacy risks that need to be addressed, Sun says. For example, privacy impact assessments and security risk assessments should be conducted during

the design phase, while regular monitoring and testing should be conducted during the deployment and maintenance phases.

What Happens With Data

Another area organizations may overlook is establishing clear policies and procedures for collecting, using, and sharing data, Sun says. “Organizations should be transparent about their AI systems, including how they work, what data they collect, and how that data is used,” he explains. “They should establish accountability measures to ensure that AI systems are used ethically and fairly and should be transparent about incidents and breaches if they occur.”

Internal auditors need to understand how AI technologies use data, “rather than just think about what data goes in and what data comes

out,” says James Gerber, CEO at Boston-based cybersecurity company SimSpace. “The lack of traceability around AI is probably the most problematic issue for companies to try to come to terms with, especially if personally identifiable information is involved as part of the process.”

For example, CAEs should ask how the data is used and where it goes. Does the developer keep it? Does the developer use it to create other systems? Is the data shared with competitors or other vendors? Is it deleted?

“Companies must realize they are just as liable for any data misuse for their use of the technology as the tech firms developing the systems are,” Gerber says. “They should also be aware that in many jurisdictions there is no legal requirement for tech firms to sandbox their products (whereby developers test their products with regulators to check they are compliant before launching them) and that many developers still fail to ensure products are built



“Organizations should be transparent about their AI systems, including how they work, what data they collect, and how that data is used.”

—Darron Sun, Head of IT,
Hong Kong Housing Society



“Companies must realize they are just as liable for any data misuse for their use of the technology as the tech firms developing the systems are.”

—James Gerber, CEO,
SimSpace

with ‘privacy by design and default’ from the outset.”

Organizations should ensure privacy and security are considered throughout the entire AI development life cycle, Sun says. These considerations should include conducting privacy impact assessments and security risk assessments as well as implementing security and privacy by design principles.

“Mitigating the risks associated with AI technologies requires a proactive and holistic approach to cybersecurity and privacy” that combines technical, organizational, and human-focused measures, Sun says. “By taking these practical steps, organizations can reduce the risk of cybersecurity and privacy incidents, protect the integrity and trust of their AI systems and processes, and ensure the ethical and fair use of AI technologies.”

Risk Awareness

Another common mistake, Sun says, is over-reliance on

technical solutions such as encryption and access controls to mitigate AI cybersecurity risks instead of addressing the main culprit — lack of employee training or AI-risk awareness. “Organizations need to implement organizational and human-focused measures, such as employee training and awareness programs, to ensure that individuals are aware of the risks associated with AI technologies and know how to respond to potential threats,” he says.

Many organizations have embraced the use of AI chatbots such as ChatGPT and continue to allow their use even though significant risks associated with the technology have become well known. Chatbots can make phishing attacks easier, create error-free fake accounts on social media platforms, and even rewrite viruses to attack other programming languages.

Meanwhile, ChatGPT stores everything that is typed into it — including both questions and user

information. “If all that information falls into the wrong hands, the consequences could be catastrophic and have a global impact,” says Stuart Poole-Robb, CEO of London-based strategic intelligence and risk management consultancy KCSGE.

Once employees are using AI tools in the workplace, it is difficult to restrict access to them, says Leon Teale, senior penetration tester at cybersecurity vendor IT Governance in Lytham St. Anne’s, U.K. “For instance, how do you stop Frank in Sales from accessing the payee details for his colleagues?” he asks. “This would come down to fine-tuning every part of the work data available to ChatGPT and providing lists of who can access what — which is an ever-fluid area.”

One solution is to be very selective about the type of AI tools the organization uses. Major companies including Amazon, Apple, Citigroup, Samsung, and Verizon have banned employees from using ChatGPT. Razzaque

“How do you stop Frank in Sales from accessing the payee details for his colleagues? This would come down to fine-tuning every part of the work data available to ChatGPT and providing lists of who can access what — which is an ever-fluid area.”

—Leon Teale, Senior Penetration Tester, IT Governance



recommends organizations opt for AI models that are resilient against attacks and implement techniques, such as adversarial training and anomaly detection, to enhance the resilience of AI models. They also should perform detailed vendor

checks when outsourcing AI-related services, he says.

Mark James, a consultant at data privacy specialist DQM GRC in High Wycombe, U.K., agrees that internal auditors “need to ensure that the chatbot application they are using has encrypted interactions to prevent unauthorized access by third parties.” He recommends that organizations only use chatbots from trusted sources and avoid sharing sensitive information such as passwords or financial information through chatbot conversations. “This should ensure a private and secure experience,” he says.

Pruning the Data

Internal auditors may want to advise management to rethink its data retention policies to improve cybersecurity. Any AI that depends for its effectiveness on having access to all of an organization’s data repositories needs to be scrutinized to be sure how the data might be used and where it will be

“Only collect the information you actually need, only retain what is useful, and only keep it for as long as it is needed.”

—Will Richmond-Coggan, Partner, Freeths

shared, Richmond-Coggan says. “We have already seen some technology companies caught out by having uploaded commercially sensitive information into public AI chatbot tests,” he says, “leading to that information being made available to third parties, including the company’s competitors.”

Good data hygiene is crucial, Richmond-Coggan warns. “Only collect the information you actually need, only retain what is useful, and only keep it for as long as it is needed,” he advises. “Also, be robust

about enforcing erasure at the end of retention periods.”

David Helberg, director, Internal Audit and Corporate Ethics at Cameco Corp., a Saskatoon, Alberta-based uranium mining company, says organizations must review their data retention and security practices as AI adoption grows. “Generative AI demands more and more data to improve its outputs, but

this is counter to key legislation such as the General Data Protection Regulation and California Consumer Privacy Act, which call for data minimization,” he explains.



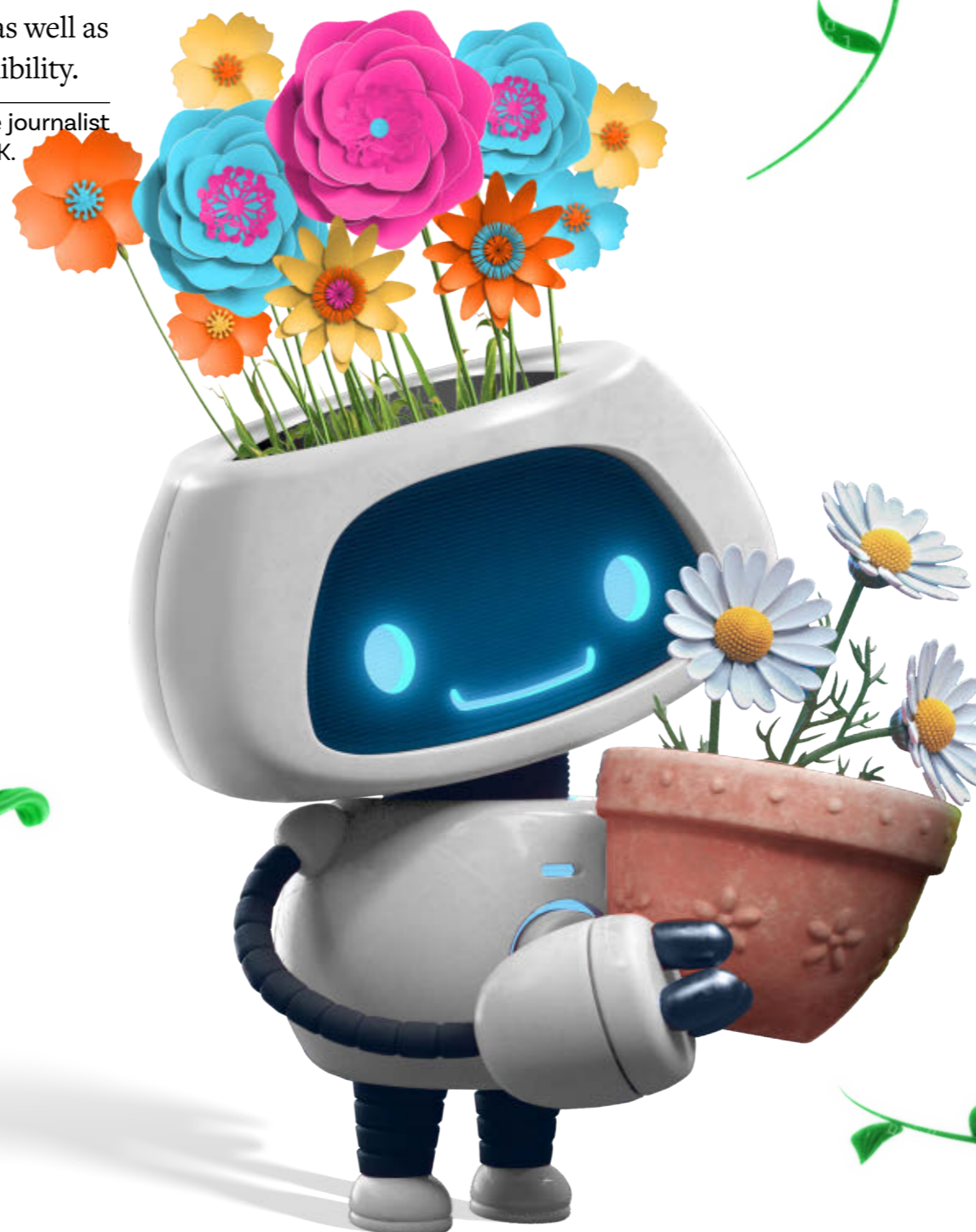
And the more data organizations have, the more they are at risk if bad actors gain access to it. “Companies must distinguish what data they must have from the data they’d like to have because the loss of substantial amounts of corporate and personal data through an AI-based adversarial attack could be catastrophic,” Helberg says.

Care of Cyber Risks

There is no doubt that AI is an invaluable tool, but internal auditors need to be aware that their organizations are responsible for identifying and managing the risks inherent in the technology.

A successful cyber hack of mountains of data inputted into AI systems will result not only in costly fines around the globe, but also substantial compliance costs — as well as a serious dent in credibility.

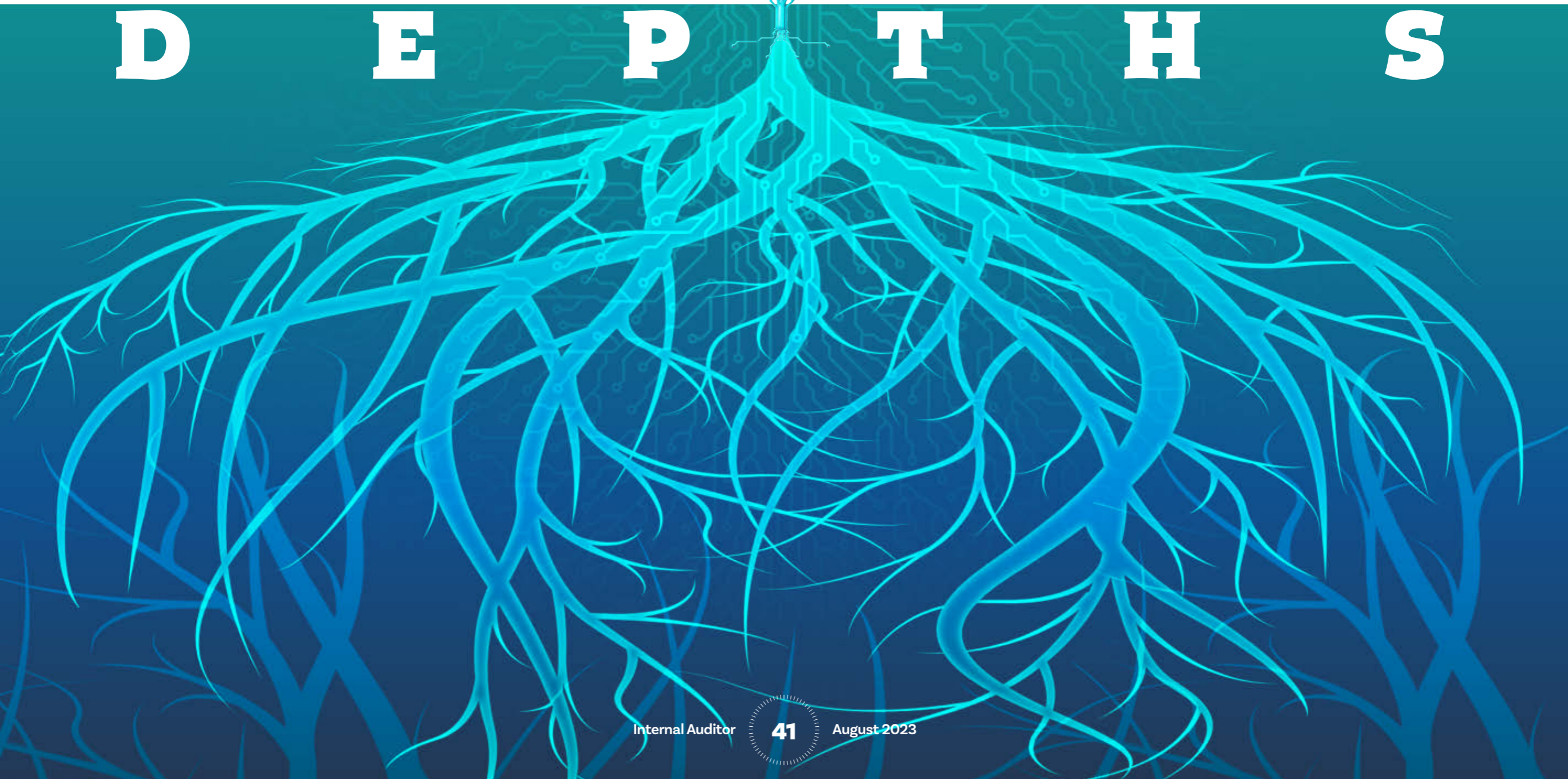
Neil Hodge is a freelance journalist based in Nottingham, U.K.



The asymmetry of cyber risk makes it difficult to detect what's lurking below the surface.

James Bone

H **I** **D** **D** **E** **N**
D **E** **P** **T** **H** **S**



Cyper risk is one of the most complex risks facing organizations, and it continues to grow unabated despite regulatory mandates and the millions of dollars spent to combat it. Academic researchers and chief information security officers (CISOs) have attempted to quantify the probability and cost of cyberattacks using various methods; however, a lack of credible data makes it difficult to calculate potential impacts or to develop a consistent tool or methodology to stop the spread.

The inherent asymmetry of cyber risk reduces proactive insights into the threats and vulnerabilities that lead to data breaches and compromised systems. In other words, cyber risk is hard to detect in a virtual environment because the threat can be hidden for months and even years from human perception. Systems can be manipulated to conceal an invasion and these approaches evolve faster than smart detection systems can keep pace.

Risk asymmetry is similar to war games, where one opponent has a unique advantage that requires the other to counter the advantage with innovative approaches to successfully defend itself. The challenge in cybersecurity is there isn't just one opponent, and the level of

sophistication in each attack cannot be judged in advance. This level of risk asymmetry creates blind spots that require internal audit to develop a comprehensive understanding of the weaknesses and vulnerabilities across the enterprise.

A COSTLY, COMPLEX RISK

A recent report from the RAND Corporation found that, globally, “cybercrime has direct gross domestic product (GDP) costs of \$275 billion to \$6.6 trillion and total GDP costs (direct plus systemic) of \$799 billion to \$22.5 trillion (1% to 32% of GDP).” The RAND study used several models to estimate the cost of a breach with varied assumptions and provided an interactive

spreadsheet to allow readers to adjust estimates for themselves. According to the study, Estimating the Global Cost of Cyber Risk, the cost of cyber risk is growing at a 15% compound annual growth rate.

What can auditors do to protect organizations from cyberattacks? Traditional audit procedures may be inadequate to detect, correct, and prevent serious cyber risks without new tools to understand the nature of asymmetry in cyber risk. This does not mean that a focus on fundamental controls such as authentication and authorization, access controls, and other audit procedures are less important. It means that more enhanced procedures are needed to understand risks related to cyber threats.

THE ROOT OF THE MATTER

To put the threat in perspective, IBM's Cost of a Data Breach reports the average time to detect and contain a ransomware attack is 326 days. The average time to detect and contain a destructive attack is 324 days, and the global average to detect and contain a breach is 277 days. These findings suggest that serious cyber threats are going undetected for almost one year, and mitigation takes nearly three months. This can lead to massive disruption, huge mitigation costs, and scrutiny from law enforcement, shareholders, and customers.

These findings beg the question, which asymmetric risks in cybersecurity are the root cause of

vulnerabilities and data breaches? According to *The Three Most Common Causes of Data Breaches in 2021*, by *Dark Reading* magazine, a publication that leverages data from the Identity Theft Resource Center, the root cause of data breaches falls into four categories: cyberattacks, human and systems errors, physical attacks, and other (unknown). Each category has subcategories that point consistently to human error and poor decision-making about cyber risk. For example, under cyberattacks the leading causes/attack vectors are:

- Phishing.
- Smishing (using text messages or messaging apps).
- Business email compromise.
- Ransomware.
- Malware.
- Non-secured cloud environment.
- Credential stuffing (stolen credentials).

Human and systems errors include failure to configure cloud security or misconfiguring a firewall. With physical attacks, data loss is equally attributed to accidental disclosure, device theft, and improper disclosure. Each of these security failure categories are well known, yet they continue to provide attackers new opportunities to compromise systems. Fortunately, each of

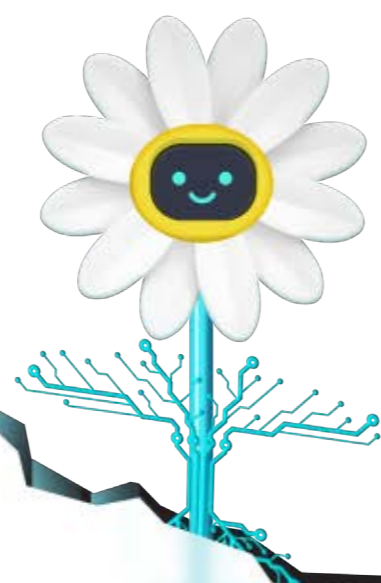
D I G G I N G D E E P to Assess Asymmetric Risk

The information security and asymmetric risk assessment process involves a deep dive into the organization's assets, risks, and mitigation efforts.

- Identify the organization's most important data and IT assets for enhanced security control measures.
- Define levels of materiality in IT control failure that would cause the greatest impacts to operations, and develop plans to address each level prospectively.
- Document and monitor known security threats but plan on residual threat risks that are not yet known.
- Define human risk factors: human error, insider threats, executive exposure, decision error, social media, workflow design, and manual processes. Map them to perceived vulnerabilities for mitigation.
- Define human risk factors as key performance and risk indicators.
- Define the human-machine risk vectors (critical systems, data, assets, third-party, and social media) to estimate potential exposure to breach.
- Quantify, as possible, the probability of system exploitation. Include confidence levels of assurance (0-100%). *Note: Zero risk or zero IT failure is unrealistic and sets the wrong expectation.*
- Consider a “zero-trust” approach and methodology that fits the risk posture of the firm.
- Consider two to four scheduled disaster recovery tabletop exercises under different scenarios a year.
- Conduct multiprong attack scenarios that include simultaneous events and single-event attacks.
- Plan IT security posture based on risk appetite in alignment with management expectations and operational effectiveness.
- Clarify the specific type of risk being reduced. Is it the risk of noncompliance or the risk of a data breach? This allows auditors to determine the effectiveness of controls for each type.

SOURCE: UPGUARD, HOW TO PERFORM A CYBERSECURITY RISK ASSESSMENT (2023 GUIDE), MAY 21, 2023

By enhancing audit procedures and recognizing asymmetry in audit practices, internal audit can better address the human factors in cybersecurity.



these areas can be positively impacted by auditors with the right mindset.

THE HUMAN FACTOR

There appears to be a disconnect between the continued rise in cyber threats and prescriptive approaches in cybersecurity, risk, and audit to mitigate the threat. That disconnect is in how auditors and CISOs identify key cyber risks to influence the right behaviors and reduce data breaches. By enhancing audit procedures and recognizing asymmetry in audit practices, internal audit can better address the human factors in cybersecurity.

Enhance audit procedures. The airline industry is a pioneer in human factors and has applied these concepts to manage the risk of transporting millions of passengers from point A to point B safely, given the probability of equipment failure, weather conditions, bird strikes, pilot fatigue, and varying skill sets. The airline industry didn't use a risk framework; instead, it studied the pilot's dashboard, workflow, and navigation systems, and added a co-pilot to support the pilot. These approaches to enhance "situational awareness" may not be included in the audit toolkit but should be.

It should not be surprising that situational awareness is also needed

in cybersecurity. Cybersecurity professionals have adopted the concepts from human factor science aeronautics for the same reason: to manage uncertainty.

A pilot, auditor, or CISO must respond and adapt to events in real time to ensure the mission is completed. Auditors should understand the level of situational awareness the IT team has. Is there visibility into a complete inventory of critical assets? Does the disaster recovery plan include contingencies for an outage or ransomware attack? Is the workforce distracted with manual processes and administrative projects? Is the workforce trained on social media and social engineering risks?

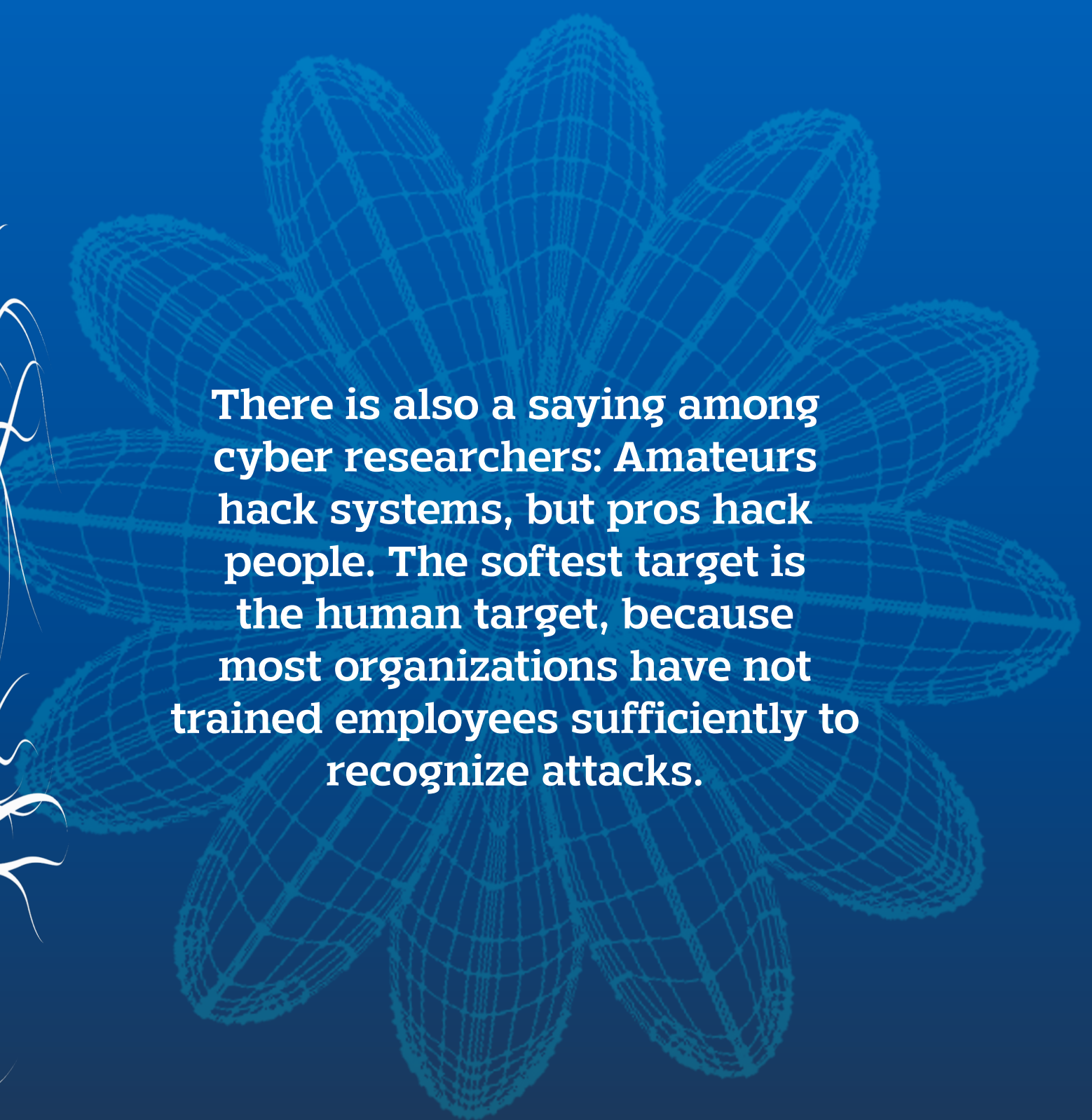
Auditors need to develop more insightful questions to better understand the gaps in situational awareness in cybersecurity. To understand the importance of situational awareness in cyber risks, auditors must know how to recognize asymmetry.

Understand asymmetry in audit practice. The goal of asymmetric cyber risk management is to make a data breach as difficult and costly as possible for the attacker. Cyber criminals are like car thieves. They start by checking the car doors to see if they are unlocked or for the keys

in the glovebox. Attackers seek easy access and low-cost approaches, which is why phishing attacks and ransomware are common weapons of choice.

There is also a saying among cyber researchers: Amateurs hack systems, but pros hack people. The softest target is the human target, because most organizations have not trained employees sufficiently to recognize attacks. Attackers commonly conduct research on a target firm by studying publicly available information. Next, attackers will start with social engineering at the receptionist level, or if they have acquired emails of employees on social media sites, they may make random calls posing as vendors or customers and asking what may seem like benign questions.

This tactic was demonstrated during a live performance at a cybersecurity convention in Las Vegas, where social engineer presenters entered a sound-proof booth and called target firms that were randomly selected before the convention. Each attacker developed a persona before the call with a checklist of information to gather. Some attackers posed as IT staff at the firm conducting tests. Others tricked



There is also a saying among cyber researchers: Amateurs hack systems, but pros hack people. The softest target is the human target, because most organizations have not trained employees sufficiently to recognize attacks.



the receptionist or random employees to click on a false link.

These presenters demonstrated that a calm voice and benign questions can disarm staff to divulge key insights into a firm's security posture. Factors such as how much training the employee has received or how helpful he or she is during the call can determine the likelihood of a breach. One stolen email credential may be all the attacker needs.

The attacker presenters were stopped in their tracks when the targets asked for information only in-house employees would know or were skeptical in providing information without validation.

Many attacks start with quiet surveillance operations at the human level and move to more advanced attacks once the attackers determine the most effective way to

proceed. That is risk asymmetry in real time. Ransomware, chatbots, and phishing get all the attention in the media, but the real attack may have happened months or years before with simple approaches — person to person.

The same approach occurs at the systems level virtually. Attackers are routinely searching for zero-day vulnerabilities, email credentials, and profiles of executives whose information is publicly available. If auditors think these are not the risks they thought they were managing, they are not alone.

The enterprise is no longer a hardened shell, but is virtual, which is why enterprise risk is no longer a valid approach to risk management. Thinking like a hacker gives auditors insight into the unanticipated ways the organization is exposed.

PUT IN THE EFFORT

Creating simplicity in cybersecurity is the hardest thing to do in any organization, but the effort pays dividends in reducing cyber risk asymmetry. Designing simplicity into cybersecurity means that auditors must understand the pain points inherent in situational awareness and impacts on security teams to manage risks. The goal of reducing complexity of operations requires innovative IT service level agreements (SLAs) between each of the three lines of the organization. SLAs must include explicit agreed-upon tradeoffs between risk-based cybersecurity and organizational objectives.

James Bone is executive director and founder at GRCIndex in Lincoln, R.I.



Ransomware, chatbots, and phishing get all the attention in the media, but the real attack may have happened months or years before with simple approaches — person to person.



Mobilizing a Cyber Risk Strategy

Today's cybersecurity strategies must address the business risks introduced by digital transformation, remote working, and a larger digital infrastructure.  Daryl Pereira

Digital transformation happened fast for many organizations. One major driver was the lockdowns during the COVID-19 pandemic. During this period, many consumers turned away from brick-and-mortar establishments in favor of online vendors offering new ways to purchase goods and services, conduct financial transactions, work, and play.

As businesses and governments focused on establishing or expanding their online presence, it sparked a change in traditional business models and supply chains, with digital transformation becoming a must-do to survive. New mobile apps and online services appearing during 2020 and 2021 covered a broad range of human interaction — from food delivery and shopping,

to entertainment, to doctors' visits (telehealth). As a result, the digital footprint of most homes and businesses — the record of their online activities — expanded by a factor many times larger than before COVID-19. Figures from the International Trade Administration offer some perspective: In the wake of the pandemic, global e-commerce revenue grew by 28% in 2020 and 34% in

2021, compared to the forecast growth rates of 9% and 12%, respectively.

In the wake of such growth, organizations have struggled to secure their digital assets, with cybersecurity investment lagging behind digital transformation investment. All of this has led to a cyber-risk gap, as organizations try to secure their resources with the same level of cybersecurity investment as in the pre-COVID era. The rise of successful and damaging cyberattacks in the past four years bears witness to this gap.

To address this issue, internal auditors have begun looking at cyber risk as not just an IT risk but a business risk. Audit functions have shifted focus from auditing the usual suspects of IT hardware and software to auditing critical business activities that rely on technology. To be successful, internal audit needs buy-in and involvement from the C-suite and senior business leaders, as well as other

team members who can help the organization understand the consequences posed by a cyberattack.

Gathering the Team

Over the last four years, cyberattacks have surged, disrupting daily business operations, causing reputational damage and loss of clientele, and resulting in significant impacts to organizations' profits and operations. In the Allianz Risk Barometer 2023 survey, cyber incidents and business interruption tied for the “most important global business risk” for the second year in a row, each garnering 34% of the vote among risk professionals.

While many organizations now consider cyberattacks to be a business risk, the management and audit of cyber risks is still approached as a topic for the IT department and often not assessed in terms of other business drivers.

Although internal audit does need to continue to

Audit functions have shifted focus from auditing the usual suspects of IT hardware and software to auditing critical business activities that rely on technology.



consult with operations and IT staff, it must throw a much wider net to include executives and specialists from legal, compliance, human resources, public relations, and business continuity. This enables the audit function to have a more holistic understanding of the organization's cybersecurity strategy and risks. To assess the cyber risks, internal audit needs to understand what is likely to be attacked and why; how an attacker might strike; how a cyberattack could affect business operations; and what might be the reputational and financial impacts of an attack.

Shaping the Cybersecurity Landscape

There are different ways to conduct a cybersecurity audit. Some audits review technical IT controls, while others focus on compliance with cybersecurity standards or frameworks. A more optimal approach combines a strategic review of business, operational, and IT risks

with a structured control methodology based on an authoritative cybersecurity framework. Internal audit can do this by reviewing the organization's cybersecurity strategy or cybersecurity plan, in addition to the usual IT and technical controls.

Stratify cyber risks. A first step in understanding the organization's cybersecurity strategy is to classify its cyber risks. To do this, internal audit needs to interview leaders and review company business strategies to understand the organization's risk tolerance in relation to its goals and vital functions. The business units that enable current and future business operations — in particular, those that rely on technology and data — are where the cyber risks will be concentrated. This will be different from organization to organization. For instance, the cyber risks will be quite different between an organization that stores its data on premises versus one that stores its data in the cloud.

The business units that enable current and future business operations — in particular, those that rely on technology and data — are where the cyber risks will be concentrated. This will be different from organization to organization.

Identify the “crown jewels.” To determine the organization's most crucial technology assets, internal audit must first consider how the organization could be damaged by a cyberattack. It must then identify the business operations that are most important and therefore key to keeping the organization up and running. These key operations in many cases will rely upon technology in some way. For example, organizations may rely upon technology for their financial transaction systems, order processing systems, manufacturing systems, or data analytics systems.

Next, internal audit should identify the sensitive data; the systems that store, transmit, and process this data; and the underlying network and hardware infrastructure that keep the key business operations functional. These are the crown jewels — a

combination of data, software, and hardware. No expense should be spared in protecting these assets.

Adopt a cybersecurity standard. The two established global cybersecurity standards should be the foundation for a cybersecurity audit program. Adopting either the U.S. National Institute of Standards and Technology's (NIST's) Cybersecurity Framework or ISO/IEC 27001 Information Security Management Systems can help auditors define the control objectives for their program. Of note, NIST provides a framework for auditing the five critical elements of a cybersecurity strategy, which are identify, protect, detect, respond, and recover.

Covering More Ground

To go beyond the traditional IT audit focus, internal audit should review the full range of cyber risks across the enterprise. Specifically, there are six business domains that a cybersecurity audit should cover.

Leadership and Governance. Within this domain, internal audit assesses whether management is demonstrating due diligence, ownership, and effective risk management. Audit objectives should begin with understanding how management has defined ownership of its cyber risk program, the governance structure for cybersecurity roles, and responsibility for each business function.

Internal auditors should look at how management has defined and identified its sensitive data assets. Further, they should review how management has inventoried third-party supplier relationships and assess the organization's current cybersecurity capabilities. Management should define a cybersecurity strategy and approach for how much investment should be made in terms of people, process, and technology. Finally, auditors should understand how the board and executive management are educated

on current cybersecurity concerns and cyber risk management solutions.

Human Factors. In this second domain, internal audit should assess the level and integration of the security culture and whether it empowers and ensures the right people, skills, culture, and knowledge. The culture and expectations should be defined and supported by training and awareness

programs, and the organization should have personnel security measures in place. Moreover, auditors should determine whether the organization has defined its talent management and developed specific learning paths for key personnel. For instance, IT personnel should not be asked to perform both IT and cybersecurity roles without adequate specialist training.

Information Risk Management. The third domain focuses on how well the organization achieves comprehensive and effective risk management of information for itself and how it ensures these standards are upheld by delivery and supply partners.

Internal auditors should assess how the organization identifies and communicates risk tolerance. It is important to review how

Auditors should determine whether the organization has defined its talent management and developed specific learning paths for key personnel. For instance, IT personnel should not be asked to perform both IT and cybersecurity roles without adequate specialist training.



management has linked identified cyber risks to each sensitive data asset, the robustness of the risk assessment methodology, and the metrics used to measure risk. Additionally, internal auditors should look at how management assesses third-party supplier accreditation for the supply of IT systems, hardware, software, and managed IT services.

Business Continuity and Crisis Management. Within this fourth domain, internal audit should ensure the organization is prepared for a security event and can prevent or minimize the impact through successful crisis and stakeholder management.

This involves looking at how management assesses its ability to manage cyber incidents and whether it performs an analysis of operational risks and financial requirements that may occur because of an attack.

Management should have robust business continuity plans based on different cyberattack scenarios. For

example, the response to a ransomware attack is different from the response to a denial of service attack where key IT systems and infrastructure are taken down by attackers, causing operational disruptions or massive system downtime. Internal auditors must understand how resources have been assigned and trained to execute the business continuity plan for cyberattack scenarios. A written plan is insufficient unless all personnel are trained in their respective roles and responsibilities.

Moreover, it is important that management regularly tests the business continuity and crisis management plans. Internal auditors should understand how the crisis management plan integrates with corporate communications, as one of the best ways to prevent reputational damage in a crisis is by planning how to handle queries from the media, regulators, the board, employees, and other stakeholders.

IT and Operations. In this fifth domain, internal audit assesses how control measures are implemented to address identified risks and minimize the impact of compromise. Audit objectives for this domain begin with reviewing how management has cataloged all relevant cybersecurity compliance requirements and linked those requirements to cyber controls within the organization. It is important to include all risk relating to technology, privacy, data governance, third parties and outsourcing, business continuity, and security regulations when assessing this domain.

Internal audit should review how management performs threat and vulnerability management and security operations monitoring, both of which are crucial to prevent and detect potential pathways for cyberattacks. By assessing cyber-incident response capabilities, auditors can help the organization determine if it would be more advantageous to retain

Management should have robust business continuity plans based on different cyberattack scenarios. For example, the response to a ransomware attack is different than the response to a denial of service attack.

a third-party provider with proven expertise.

Another audit objective is to understand how the IT department builds systems and whether program code is written under a secure software development life cycle. Finally, auditors should review whether the cybersecurity activities are integrated with the broader IT service management activities, or whether IT and cybersecurity capabilities are running in operational silos.

Legal and Compliance. Internal audit should consider which regulatory and international certification standards are relevant to the organization's sector.

Audit objectives for this sixth domain begin with understanding how management has selected and implemented an IT control framework and implemented logical and physical security controls. Additional audit considerations include whether cybersecurity is formalized as a standing agenda item for the audit



committee, whether management is monitoring litigation and cyber event trends, and whether the organization needs cyber insurance.

Making the Cut

The cybersecurity strategy of organizations must evolve to address the business risks introduced by digital transformation, remote working, and escalating cyberattacks from a larger digital infrastructure. Cyber risk knows no boundaries and permeates across business, operations, and IT functions, but internal auditors can play a role in breaking down barriers between departments.

Auditors can help promote “cyber resilience by

design,” wherein good security controls are built into systems and processes from the start, rather than bolted on during or after the development phase. The board should make itself accountable to fostering this culture by ensuring that cyber risks are understood, cybersecurity plans are well-designed, and coordination among teams is effective.

The pandemic has forced organizations to question the assumption that their supplier and partner ecosystem is operating as normal. Organizations need to revise and test resilience planning processes, equipping crisis management teams with the skills to manage under

intense pressure. Organizations need to review the definition of a worst-case scenario in this new reality and take an “assumed breach” mindset. This means that everyone should understand that a cyberattack is imminent, and plan ahead and be ready for when an attack happens — the secret to becoming a cyber-resilient organization.

Daryl Pereira, CISM, CISA, CRISC, CPA (Australia), is the Asia-Pacific leader of the Office of the Chief Information Security Officer at Google Cloud in Singapore.

Cyber risk knows no boundaries and permeates across business, operations, and IT functions, but internal auditors can play a role in breaking down barriers between departments.



think different.

The IIA's 2023-2024 Global Board chair, **Sally-Anne Pitt**, says a shift in perspective will set the stage for the future of internal auditing.

📷 Humdinger



Just over 25 years ago, one of today’s most recognized brands released a bold new advertising campaign, marking its launch into a new era of creativity and groundbreaking ideas. The slogan, “think different,” signaled the company’s efforts to reinvent itself with a focus on innovation. At the same time, it encouraged consumers to embrace individuality, question the status quo, and expand their horizons. The campaign included a series of TV advertisements that showcased influential figures from various fields known for pushing the boundaries of convention. The company, of course, was Apple Inc., which has since become one of the most innovative and valuable organizations in the world.

As a profession, internal auditing has reached its own “think different” moment — and that’s why I’ve chosen this phrase as the theme for my tenure as chair of The IIA’s Global Board of Directors. We face a host of challenges and opportunities that require new ways of looking at things. With increased interconnectedness around the globe, a continually evolving risk landscape, rapid evolution of technology, and ever-changing stakeholder expectations, we must

position ourselves for the future and be willing to explore new ideas.

I see four fundamental areas, in particular, where we need to “think different”: the way we collaborate, the skills and backgrounds we bring to the table, the perspectives we offer, and how The IIA operates as a global organization. By embracing an expanded mindset across these areas, we can unlock new possibilities and forge ahead in a world that demands adaptability.

different relationships

While internal audit on its own can be a powerful asset, we can enhance our impact by exploring collaborative

opportunities with other functions. We should be aware of what assurance providers across the organization are doing and look to coordinate with them where potential synergies exist. Developing relationships with second-line units, in addition to management, can help us better understand where the risks and opportunities lie.

Of course, independence remains a core tenet of our profession. But to an extent, we may have hidden behind concerns about independence to the point where it constitutes a disservice to clients. We need to be careful not to completely separate ourselves from the business, as too much distance can limit our ability to understand what’s happening in the organization and which areas may require our attention.

Excessive emphasis on independence, in other words, can actually diminish the value we add. And it can deprive the organization of the skills, resources, and benefits we offer as a profession.

The key is to achieve the right balance. We need to collaborate and build relationships, without being compromised by them. We need to rethink our place in the organization and how we interact with stakeholders at all levels. And we need to adopt a fresh perspective on how best to deliver value, what information and resources are required to get there, and how we can better align our efforts with organizational needs. By doing so, we can better position ourselves as strategic partners and help ensure the organization’s long-term success.

We face a host of challenges and opportunities that require new ways of looking at things. ... We must position ourselves for the future and be willing to explore new ideas.

different skills and backgrounds

Another way to enhance the level of service internal audit provides is to make sure our expertise and skills match organizational demands. The most effective way to deliver

value can vary significantly from one organization to the next — we need to be mindful of that as we look at talent management within our teams.

For example, suppose you're creating an audit department within a newly formed government agency.

Before it becomes operational, the agency needs to focus on building systems and processes, hiring staff, creating frameworks, defining objectives, and so on. The most relevant audit services in that circumstance would likely be more traditional in nature and focused on the control

environment. Therefore, meeting stakeholder needs does not necessarily mean bringing the latest, most cutting-edge skills to bear. At the same time, you probably wouldn't want a large, well-established organization with a complex risk profile to rely on an audit function composed mostly

different points of view

We also need audit functions with the right mix of perspectives; otherwise, we may fail to fully grasp the unique challenges of our stakeholders. For example, if a team consists entirely of individuals from the same cultural background, then it may be difficult for internal audit to effectively serve an organization whose client base comprises culturally and linguistically diverse communities.

To ensure audit functions possess the type of thinking and approach that best suits the organization, we need audit leaders who appreciate the value of diversity — those who can assemble teams with far more than one common set of experiences. The process should involve consideration across multiple dimensions, including diversity of thought, worldview, background, and culture.

Diversity makes good business sense; it helps bring a variety of perspectives to problem-solving and enhances creativity. And the more creative we are, the more likely we are to innovate and develop unique solutions. Teammates can benefit professionally from diverse teams by receiving exposure to approaches and ideas different from their own.

of compliance-focused auditors. To ensure our relevance and value, internal audit's expertise needs to align with the organization's unique priorities, risks, and business environment.

Where we draw that expertise from also merits some rethinking. As a consultant, I work with audit functions that serve large mining and engineering organizations, and I see that hiring managers often look to the client industry for talent needs. Many of their teams include practitioners who come from engineering or mine remediation backgrounds, rather than auditing or accounting. And that type of expertise is often exactly what's needed for internal audit to best serve those organizations.

The same thinking should apply to whatever industry or type of organization we work in. That doesn't mean health-care auditors need to be medical experts or that financial services auditors need to be bankers — but they should have enough understanding of the business to make meaningful contributions. And while sourcing expertise outside the organization — or insourcing through the use of guest auditors — may be a viable option, the core internal audit team still needs to have sufficient knowledge and expertise.

Diversity makes good business sense; it helps bring a variety of perspectives to problem-solving and enhances creativity. And the more creative we are, the more likely we are to innovate and develop unique solutions.

It's also desirable from an equity and fairness perspective, as attention to diversity can help create space for different people to be involved in opportunities they haven't been historically. And ultimately, we will be a stronger profession with a greater variety of people participating in it (see "A Spectrum of Talent" on page 59).

a new and different vision

Recognizing the need for internal auditors to adapt and change, The IIA also must evolve to provide relevant guidance and support to its members. The Global Board is committed to actively engaging with internal auditors to understand what they need from their association. We'll look to better gauge what's important to you, what you value, and what assistance you're seeking to help meet stakeholder expectations. That involves making sure we understand what's relevant to specific countries and regions — and not just applying a one-size-fits-all approach across the globe.

The IIA's affiliate structure spans more than 100 countries — and we will continue to leverage that

it's about the journey

My career path has been an exciting one, winding through numerous roles and challenges. After receiving a master's degree in public policy, I worked with remote Aboriginal communities through public sector health and housing agencies in central Australia. I later moved to Darwin, where I served in various government roles for nearly a decade, eventually leading to a position at a public sector risk and audit function.

Although I never intended to make a career of internal auditing, it led to my husband and me establishing our audit consulting business, which we've now operated for 20 years. We work across two key areas: performance audits in government agencies and internal audit quality and capability building across both the public and private sectors.

Outside of my professional activities, I enjoy the outdoors, especially cycling. My husband and I love soaking up the cafe culture and visiting craft breweries within riding distance. We live in the inner city of Melbourne, located near the Yara River and the Parklands — a particularly cycle-friendly area, with lots of bike paths and scenic routes to explore.

I also love travel, and I've been fortunate to visit many places outside my home country with my family as well as through my involvement with The IIA. I've especially enjoyed getting to meet people from different countries and gaining a better appreciation for unique cultures and perspectives. Just like in cycling, where the journey is as important as the destination, I have learned to embrace every moment, enjoy the scenery, and appreciate the people I have met along the way.



presence to gauge how best to serve practitioners in different parts of the world. It enables the Global Board to set a more relevant agenda and develop strategies based on priorities expressed across our diverse range of stakeholders. We're also looking at how affiliates can work together on common projects so we can better harness our collective knowledge to make enhancements broadly across The IIA.

To further inform IIA initiatives and the work of the Global Board,

The Institute has launched an ambitious effort to envision the future of the internal audit profession. The Vision 2035 Project is geared toward helping us determine what the profession will look like over the next 10 to 15 years and forming a comprehensive, integrated, and forward-looking vision. We'll use this information to help develop our longer-term strategic planning and help answer questions such as how we should deliver training, what our association means for different constituencies, what type of work practitioners should be performing, and how we collaborate with the second line. The project is a key component of our commitment to "think different," and it will play an instrumental

role in defining the internal audit profession over the next decade.

embracing new possibilities

As we reimagine internal auditing and prepare for the challenges ahead, I encourage practitioners at all levels to consider the many ways of contributing to the profession. For audit leaders seeking to hire, there are so many individuals with unique backgrounds that could further enrich the profession's talent pool. We should keep an eye out for those candidates who don't necessarily fit the internal auditor stereotype but can still add great value. And for staff and mid-level

auditors with untapped potential, your experiences and talents should not be underestimated. They can be brought to bear toward organizational problem-solving — as well as leveraged through volunteer opportunities at local IIA chapters and affiliates.

The more we celebrate our experiences and recognize our individual skills and abilities, the more value we can add as a profession. By adopting a "think different" mindset, we can embrace innovation and make a greater impact in our organizations. I look forward to seeing what we can accomplish together.

Sally-Anne Pitt, CIA, CGAP, is managing director of Pitt Group in Melbourne, Australia.



The more we celebrate our experiences and recognize our individual skills and abilities, the more value we can add as a profession.



A SPECTRUM OF TALENT

Neurodivergent employees offer hidden strengths to organizations that are inclusive of them.

◆ Christine Janesko

and values and enjoys working with her team, having fun while navigating the world of internal auditing.

But Yuen's path to a successful internal audit career was bumpy, to say the least. After discovering internal auditing through a banking internship, earning a master's degree in accounting, and passing the Certified Internal Auditor exam, the highly intelligent graduate encountered rejection after rejection due to communication missteps during job interviews.

Even after getting a handle on interviews and landing great jobs, the trouble didn't end. In one role, she was nearly fired due to the

inability to appropriately communicate; at another, she was placed on a performance review. Finally, after enduring a pattern where she would ascend in her audit roles and then descend due to communication issues, Yuen found herself lost in her career and falling into depression.

She sought help and learned she has Asperger syndrome, also known as Autism Spectrum Disorder. The disorder usually is associated with difficulty in picking up on social cues and interacting socially, a tendency to be direct and literal, anxiety, a need for structure, and hypersensitivity to certain stimuli. Like many women on the

Yuen is enthusiastic about her role at SoFi Technologies, a fintech company based in San Francisco. She is the senior director of Global Sarbanes-Oxley and Audit Compliance, managing a team of 17 employees and 15 consultants. Yuen is quick to praise the company's culture

LIKE MANY WOMEN ON THE AUTISTIC SPECTRUM, YUEN WENT UNDIAGNOSED UNTIL SHE HIT A WALL IN HER ADULT YEARS.



autistic spectrum, Yuen went undiagnosed until she hit a wall in her adult years.

“When I nearly lost my career, it was a great awakening that something was wrong,” Yuen says. “So, I met with a psychiatrist who performed testing and confirmed my diagnosis, got medicine, and began meeting regularly with a psychologist.”

Yuen is an example of someone with a neurodivergent condition who experiences challenges at work, yet can be successful with a correct diagnosis, support, and an inclusive workplace. And people like Yuen are not rare. According to *A Rising Tide Lifts All Boats*, by Deloitte, “roughly 10% to 20% of the global population is considered neurodivergent,” with

cognitive conditions such as autism, obsessive-compulsive disorder, dyslexia, or attention deficit hyperactivity disorder (ADHD).

People with brain differences often have traits that make them desirable employees, yet they also suffer higher unemployment — as high as 85% for people with autism, according to Autism Speaks Canada. Organizations that

learn to work with neurodivergent employees can greatly benefit from their hidden strengths — and gain access to a larger talent pool.

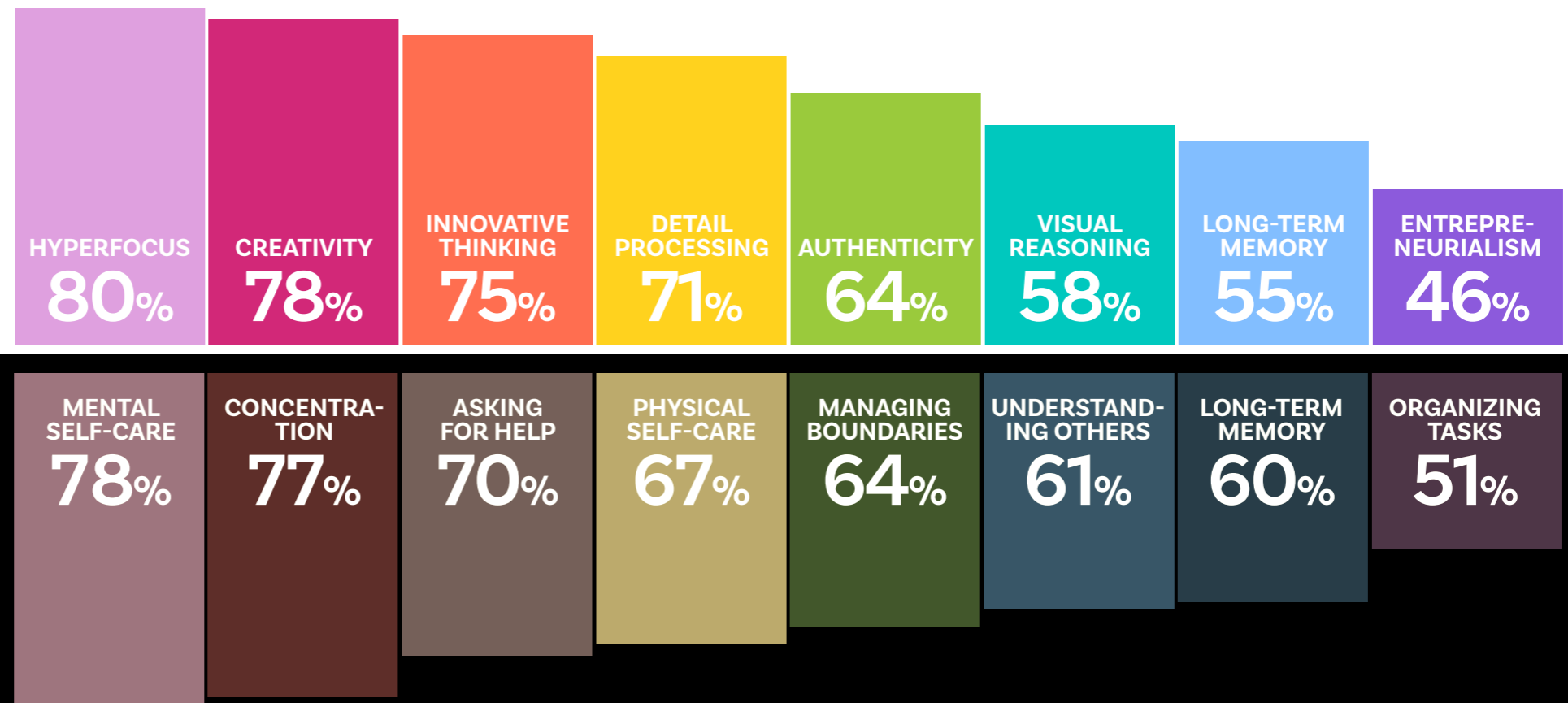
A WORKPLACE ADVANTAGE

Some organizations are starting to realize that the neurodivergent population is both overlooked and highly capable. In *Neurodiversity at*

Work 2023, a study by U.K. nonprofit Neurodiversity in Business and Birkbeck, University of London, researchers looked at both the strengths and difficulties of 990 neurodivergent workers (see “Neurodivergent Employees’ Top Strengths & Challenges” on this page). Along with challenges, employees in the study reported high rates of sought-after traits. The 127

NEURODIVERGENT EMPLOYEES’ TOP STRENGTHS & CHALLENGES

SOURCE: NEURODIVERSITY AT WORK 2023, NEURODIVERSITY IN BUSINESS AND BIRKBECK, UNIVERSITY OF LONDON.



employers who participated in the study rated their neurodivergent workers even higher for all these traits.

“Neurodivergent individuals think, communicate, and process information in different ways,” says Diana Mirakaj-Finnerty, CEO of Specialisterne USA, a global nonprofit that places autistic and similarly neurodivergent individuals and helps employers adopt neuro-inclusive practices. “These are not deficits but differences, and many of these differences are also strengths.”

Olla Jongerius, founder of Berlin-based BeamReach Inclusion, which offers corporate workshops, strategy

design, and coaching on how to attract and support neurodivergent employees, points out that the neurodivergent population is a largely untapped market. “There is a massive war for talent — especially in tech companies,” she says. “There are simply not enough qualified candidates. And not to generalize, but a lot of people who are neurodivergent have an amazing talent of analyzing data or analyzing situations — of seeing things differently.”

Yuen says employees on the autistic spectrum can be a good fit for internal audit, especially if they have support. She lists pattern recognition, problem solving, and

abstract thinking as skills many autistic people possess that can be an asset in internal auditing. These skills can help neurodivergent internal auditors more easily learn the skills needed for data analytics, for example, she says.

Another common trait is the ability to remain unemotional in the face of challenge. “Emotional detachment really makes us great auditors because we are not influenced by fear,” Yuen explains. “A lot of times, what I’ve experienced in fraud investigations and interviews is someone who is very defensive, who tries to knock you down, and says things like, ‘Who are you to

“Neurodivergent individuals think, communicate, and process information in different ways. *These are not deficits but differences, and many of these differences are also strengths.*”

—Diana Mirakaj-Finnerty, CEO, Specialisterne USA



YUEN SAYS EMPLOYEES ON THE AUTISTIC SPECTRUM CAN BE A GOOD FIT FOR INTERNAL AUDIT. SHE LISTS PATTERN RECOGNITION, PROBLEM SOLVING, AND ABSTRACT THINKING AS SKILLS MANY AUTISTIC PEOPLE POSSESS.

ask me these questions?” In these cases, Yuen says, she can easily deflect and redirect the person back to the questions.

HIDING IN PLAIN SIGHT

Jongerius, who has ADHD, is quick to explain that employers can't just hire a neurodivergent employee or diverse employees in general and expect instant innovation without some kind of culture change. Diversity and inclusion are two different things, she explains. “Diversity is a fact; inclusion is a choice. Inclusion is managed diversity.”

Jongerius sometimes uses a cloakroom analogy to

“Diversity is a fact; inclusion is a choice. Inclusion is managed diversity.”

—Olla Jongerius, founder, BeamReach Inclusion



explain the idea of inclusion. She asks: Can employees be their true selves, or do they have to leave their identities at the door, like shedding a coat? “It all goes back to organizational culture — how comfortable employees are at voicing their needs,” she says.

According to the U.K. study, many people are still not comfortable asking for help. Among neurodivergent employees, 65% say they worry about stigma and discrimination from management in disclosing their conditions or requesting support, and 55% say they worry about stigma and discrimination from colleagues.

And employers may not have the resources to help — 40% of respondents say there are no supportive and knowledgeable staff.

Even though Yuen's doctors encouraged her to disclose her medical diagnosis at work, she at first hid her condition because of the perceived stigma. She says she did not want to be treated differently.

“A lot of people ‘mask,’” says Jongerius, citing a term that describes mimicking “normal” behavior and hiding a condition to fit in. “It takes a lot of energy to wear this mask all the time. It's linked to poor mental health.”

CHANGING THE CULTURE

Yuen says she now knows what she needs to be successful in her job — things like clear instructions and agendas in meetings, honest and immediate feedback, transparency when things change, the ability to work from home and create her own workspace — and a work culture that allows her to be honest with co-workers about her neurodiversity. “I actually feel liberated when I can be my true self,” she says.

Mirakaj-Finnerty says a first step in ensuring employees feel safe enough to express their needs is making sure that disability

AMONG NEURODIVERGENT EMPLOYEES, 65% SAY THEY WORRY ABOUT STIGMA AND DISCRIMINATION FROM MANAGEMENT IN DISCLOSING THEIR CONDITIONS OR REQUESTING SUPPORT. — NEURODIVERSITY AT WORK 2023

“If you can set that culture right at the top, which is, ‘Look, we recognize that a significant portion of our folks are neurodivergent. **We want them to be able to express themselves authentically...**’ — **that, I think, is conducive to neurodivergent well-being.**”

—Dan Harris, CEO, Neurodiversity in Business



and accessibility are part of the organization’s diversity, equity, and inclusion strategy. “If they aren’t, start again, because without disability, which includes the neurodiversity umbrella, you’ve missed the point,” she says.

A second step is to educate the workplace about brain differences. “Learn from and listen to people with lived experience,” Mirakaj-Finnerty says. “There are neurodivergent employees within your organization already, so give them the opportunity to step forward and have a voice — and when they do, don’t be afraid to ask questions because that’s the

best way to discover more about someone.”

Dan Harris, CEO of Neurodiversity in Business, says honest, open communication from executives can go a long way toward making neurodivergent employees feel more accepted in the workplace. “If you can kind of set that culture right at the top, which is, ‘Look, we recognize that a significant portion of our folks are neurodivergent. We want them to be able to express themselves authentically, and we want to become more neuro-inclusive’ — that, I think, is conducive to neurodivergent well-being,” says Harris, who is diagnosed with both autism and ADHD.

A Spectrum of Talent

Taking the stigma out of self-disclosure and working with people to determine their needs also may help reduce turnover, Harris says. The U.K. study backs this up. Of neurodivergent employees who report having no accommodations, 31.5% say they are “very likely to leave” their employer within the next year, compared to only 7.8% of respondents who report having accommodations tailored to their needs.

A GLIMPSE OF SUCCESS

Some major employers have developed programs to specifically attract and retain different types of neurodivergent

MAKING IT WORK

Top 8 most helpful workplace adjustments for neurodivergent employees.

SOURCE: NEURODIVERSITY AT WORK 2023, NEURODIVERSITY IN BUSINESS AND BIRKBECK, UNIVERSITY OF LONDON.

8

TAKING MORE FREQUENT BREAKS

7

ABILITY TO CHANGE LIGHTING

6

ADAPTABLE POLICIES & PROCEDURES

continued on page 65

employees. Bank of America could be considered a pioneer in this aspect, having begun its Support Services program back in 1990. The program includes more than 300 team members with cognitive or developmental disabilities such as brain injuries, autism, or Down’s Syndrome, with an average tenure of 20 years at the bank.

Support Services Executive Mark Feinour says Bank of America partners with local agencies that work with neurodivergent adults. These nonprofits serve as both recruiters and coaches. “They are very familiar with the skills we’re looking for, the opportunities we have.

So they know what to train and coach their clients on to make them ready when we do have an opportunity,” Feinour says. The bank continues to work with the support partner, as needed, to ensure each employee is successful — even outside the workplace.

Global software company SAP is another organization committed to working with neurodivergent employees. SAP’s Autism at Work program, which began in 2013, has a cohort of about 215 autistic employees. The program provides accommodations and support to a mix of full- and part-time employees, interns, vocational trainees, and contractors who work in

technical and nontechnical roles, with no limitations on types or levels of roles.

“We believe that people on the spectrum are as capable of performing in their jobs as neurotypical people,” says Sarah Loucks, Autism at Work global lead in the Global Diversity & Inclusion Office at SAP. “Autism at Work taps into an underutilized talent source by reducing barriers of entry so that qualified individuals can fully develop their potential.”

Both Bank of America and SAP work with outside organizations to provide training and education to managers and staff who work with neurodivergent

“[Our partners] are very familiar with the skills we're looking for. ... **So they know what to train and coach their clients on to make them ready.**”

—Mark Feinour, Support Services Executive, Bank of America

“Autism at Work taps into an underutilized talent source by reducing barriers of entry so that qualified individuals can fully develop their potential.”

—Sarah Loucks, Autism at Work Global Lead, SAP



5

ABILITY TO CHANGE NOISE LEVEL

4

DUAL SCREEN OR READING STAND

3

PRIVATE WORK SPACE AS NEEDED

2

ABILITY TO WORK PARTLY AT HOME

1

MORE FLEXIBLE SCHEDULE

continued from page 64

employees. SAP offers a Candidate Experience Guide to hiring managers and recruiters that details how to create an “autism-inclusive hiring experience.”

Mirakaj-Finnerty recommends that organizations consider just these types of alternative approaches to recruitment and sourcing of candidates. Autistic people, in particular, sometimes lack soft skills that hiring managers look for in an interview — an easy smile, the ability to banter or crack a joke, and good eye contact.

“When trying to access this talent pool,

competency-based versus traditional resumes and interviews will result in far better outcomes, and far less unconscious bias,” she explains.

A WIN FOR ALL

Harris and Jongerius both assert that improving culture and being more inclusive helps all employees. “What works well for your neurodivergent employees actually enables everyone to be more efficient, more innovative and creative,” Harris says. “The organizations that are out there not just talking about neurodiversity but trying to become more inclusive — those are the organizations opening up new talent pools.”

“I may have been born with a neurological condition, but I now see it as a gift. Overcoming the challenges this gift brings gives me a desire to thrive in life.”

—Nancy Yuen, Senior Director, Global Sarbanes-Oxley and Audit Compliance, SoFi Technologies

In the case of organizations like Bank of America and SAP, they’re also changing lives. “One of the joys of my job is seeing what Bank of America has enabled our teammates to do,” Feinour says. “They’ve had the opportunity to move out of a group home and into their own apartment. I’ve seen teammates that have met here at work. They’ve gotten married. They’ve started families. They’ve bought homes.”

In presentations about her autism journey, Yuen points out that IQ is relatively permanent and static, but emotional intelligence (EQ) is fluid. People with

neurodiversities can grow and change. “EQ often may be low for us with Asperger’s,” she explains, “but with help, practice, and mindfulness, this score can improve greatly.”

Life happens, and everyone is born with unique abilities, Yuen notes. “I may have been born with a neurological condition, but I now see it as a gift. Overcoming the challenges this gift brings gives me a desire to thrive in life and seek purpose, which includes having a strong career in the work I love.”

Christine Janesko is the senior editor of *Internal Auditor* magazine.

YUEN POINTS OUT THAT IQ IS RELATIVELY PERMANENT AND STATIC, BUT EQ IS FLUID. PEOPLE WITH NEURODIVERSITIES CAN GROW AND CHANGE.



A Case for Innovation

Auditors in the Canadian government now have a tool to help ensure effective internal controls are built into innovative programs. ♦ Perla Habchi ♦ Rheya Tanner



Public sector organizations play an important role in supporting national innovation systems. Governments don't just fund and set policies for innovation programs, they actively engage with other program actors such as academia, the private sector, society, and the environment to solve issues that the government could not solve on its own. One example of these programs is the Impact Canada Program, which is a platform for bringing forward collaborative innovation ideas from actors that tackle emerging economic, environmental, and social challenges.

As these programs arise, internal audit must provide assurance that they are effectively implemented and managed. Yet, auditing innovation programs can be new territory for many government auditors, with most relevant audit methods focused on the private sector.

Government internal auditors have been on their own to identify the internal controls they should focus on in auditing these initiatives.

Recently, I conducted an extensive study to create a framework and determine the internal control areas that are essential for a public sector innovation audit. The study was based on research on public sector innovation programs around the world, interviews with program experts, and focus groups with internal auditors in the government of Canada.

The research identified six internal control categories that are essential for innovative initiatives, which form the core of the resulting framework. Five of the categories are familiar to internal auditors. Focus group participants recommended an additional internal processes component because it is at the core of successful innovation.

"The Innovation System Internal Controls Framework" on page 69 is an

evidence-based framework that provides example audit criteria, which can help shape a robust audit program. Internal auditors should determine which criteria in each of the six categories to include in engagements based on a risk-based assessment and the engagement's scope.

GOVERNANCE, MONITORING, STRATEGIC DECISION-MAKING, & OVERSIGHT

There are lines of inquiry that are specific to innovation governance, which involves partnership governance. Internal audits typically evaluate the governance structures within the innovation program organization by assessing the role of the relevant governance committees. The audit can test whether the committees meet regularly, discuss relevant topics in relation to their mandates and terms of reference, are involved in forward-looking strategic decision-making, and seek

Auditing innovation programs can be new territory for many government auditors, with most relevant audit methods focused on the private sector.

to identify risks, challenges, and opportunities.

While the governance committee's decision-making is crucial, involving relevant personnel in both internal and interorganizational committees supports information exchange and provides strategic insight for making decisions. Additionally, governance committees must be transparent in how they make decisions and establish clear roles, responsibilities, and accountabilities. Transparency allows those involved in the innovation system to perform their functions within the governance structure.

In terms of program governance, audit criteria can test whether the organization has performed a needs assessment to identify program planning materials and promote the program's continuity. The program should have planning mechanisms such as an organizational readiness assessment to better coordinate program activities. Audit criteria can

continued on page 70



Innovation System INTERNAL CONTROLS FRAMEWORK



Governance, Monitoring, Strategic Decision-making, and Oversight.

Structures and processes that ensure accountability, transparency, and strategic decision-making and how this is monitored. Strategic decision-making in this case is within the governance and organization as a whole and its flow between the actors within the innovation system.



Stakeholder/Actor Interaction and Knowledge/Information Exchange.

Interactions between the different actors within the innovation system and how knowledge and information flows among them.



Policy and Funding. Policy that enables economic stability, private investment, capability build-up, and sector-specific incentives for innovation. Governmental/public sector funding in innovation programs.

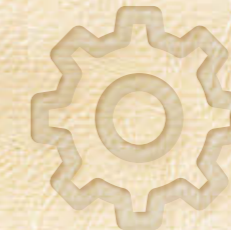


Incentives for Private Investment/Adoption.

Includes a combination of policy, funding, programs, and other incentives that encourage private sector actors to invest funds and knowledge and adopt the resulting innovation.



Intellectual Property Rights. Exclusive rights to an innovation and how that is managed within an innovation system with various actors engaging in the creation and use of innovation. Innovation should be open and provide an opportunity for licensing and commercializing.



Internal Processes. Includes finance, procurement, human resources, and tools that support and enable innovative initiatives and programs.

continued from page 68

include ensuring that the organization's overall governance follows adequate planning documents, such as guides and directives aligned with legislative requirements and partnership agreements.

Internal auditors also should consider two important aspects of innovation governance: change management and risk tolerance levels. The audit should determine whether change management mechanisms are in place to adequately accommodate for innovation. Additionally, auditors must evaluate senior management's risk tolerances, which should recognize the risks related to the nonlinear nature of innovation.

STAKEHOLDER INTERACTION & INFORMATION EXCHANGE

Innovation systems are great platforms for enabling system actors to share knowledge and information pertinent to innovation. These interactions are central

to realizing the program's intended goals and outcomes. Therefore, auditors must carefully test criteria relevant to these interactions. Does the organization collaborate with system actors and capitalize on shared knowledge and information as well as their diverse competitive advantages?

There should be an open platform where actors can share knowledge across their organizations. In addition, auditors should test whether shared information is conducive to innovative environments.

An audit should determine whether roles, responsibilities, and accountabilities are well understood and communicated to all actors. In particular, the program should closely monitor collaborations among actors who have strategic roles in advancing innovation. Communicating these relationships to senior

management can inform future partnerships with new actors entering the system.

The audit also should ensure that the organization has documented these partnerships through collaborative agreements. The program should assess the needs of external stakeholders and consider their feedback in determining investment opportunities and advancing the innovation program.

The audit must verify how the organization shares and manages the knowledge and information resulting from collaborations. Auditors should focus on whether the organization effectively communicates vital information and coordinates activities with partners and stakeholders based on this information.

The government also should have clear policies and directives that define access to information and knowledge. There should be an open platform where actors can share knowledge across their organizations. In addition, auditors should test whether shared

A Case for Innovation

information is conducive to innovative environments and whether actors share lessons learned to track results and improve decision-making.

POLICY & FUNDING

Policy and funding are the foundations for innovation. Creating supportive policy that is conducive to innovation and funding these initiatives are the biggest roles governments play in an innovation system.

Audit criteria should assess whether internal innovation policies are aligned with regulations and legislative requirements, enable competition, and allow equitable access to funds, resources, and opportunities. The audit also should assess whether innovation policies consider societal and environmental externalities and their effects on external stakeholders that are not directly influenced by the decision-making of the innovation system.

Further, these policies should encourage innovation



and sustainable growth of the innovation system where policy targets are clearly defined and communicated to all actors. Moreover, all actors must be aware of their roles and responsibilities in implementing the policy. These roles should be monitored for greater accountability.

In addition, auditors should determine whether the organization documents lessons learned from the policy results to inform future changes. Policy, in turn, should allow for the creation of programs funded through contribution agreements. The program should perform an opportunity analysis to identify investment opportunities. For these programs to work, the funding mechanisms must be transparent and equitable where selected proponents match the program requirements. The internal audit should ensure that an external firm audits a sample of project proponents regularly to ensure compliance with the contribution agreements.

PRIVATE INVESTMENT & ADOPTION

In some cases, governments do not entirely fund innovation. In other cases, they make funds available to encourage the private sector to innovate in markets it wouldn't have considered previously. Doing so also hedges some of the funding risks involved in innovation for all actors.

Some governments provide funding under a repayable contribution model, where proponents can repay the contributions when they make profits from the project. Internal auditors should determine whether the program tracks and documents these repayments.

There should be an incentive for all actors involved to adopt all resulting innovation for testing and to reveal any changes and improvements they make to it. The audit can determine which incentives are being used and how effective they are.

INTELLECTUAL PROPERTY RIGHTS

Intellectual property (IP) rights are not meant to stifle innovation within the system and are granted for the benefit of the public and industries. Therefore, resulting innovations should only be subject to IP rights mechanisms when applicable. When these IP rights are granted, the program should draft appropriate licensing agreements for actors to benefit from the innovation,

which enable cooperation in the long run.

Auditors should determine whether there are adequate controls to identify, protect, and transfer IP. The audit also should determine whether the audited organization provides employees with the tools and training to solve IP issues and identify IP.

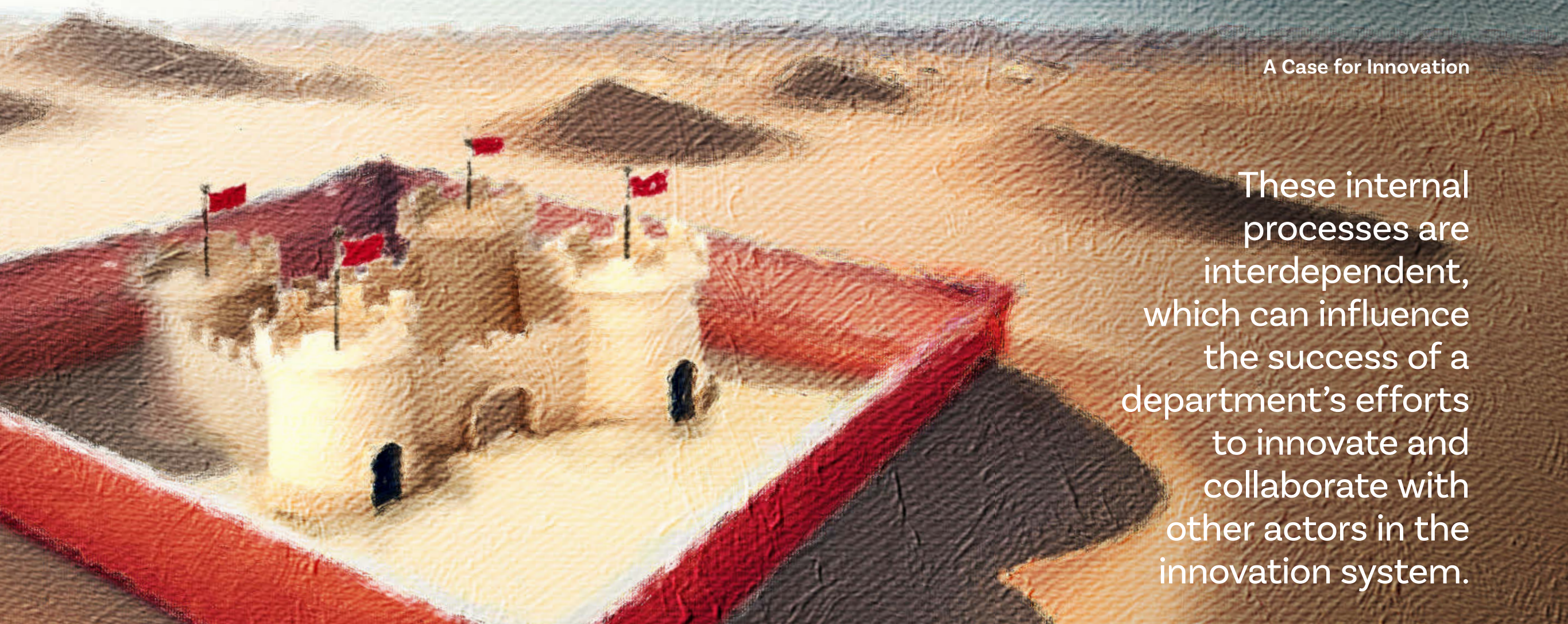
Internal scientists and employees who develop IP should have opportunities to acquire a nonexclusive license to publish their work.

In addition, mechanisms such as licensing and commercialization can promote the IP as well as the adoption of the resulting innovation.

INTERNAL PROCESSES

Various internal processes at the center of organizations enable innovation efforts. For example, a government department will need the knowledge of innovation processes and industries, procurement processes,

The program should perform an opportunity analysis to identify investment opportunities. For these programs to work, the funding mechanisms must be transparent and equitable where selected proponents match the program requirements.



These internal processes are interdependent, which can influence the success of a department's efforts to innovate and collaborate with other actors in the innovation system.

human resource (HR) management mechanisms, and financial tools to support innovation programs.

These internal processes are interdependent, which can influence the success of a department's efforts to innovate and collaborate with other actors in the innovation system. For example, the audit can examine

whether there are adequate HR mechanisms to retain talent, provide staff with knowledge and experience required for innovating, and manage knowledge transfer in support of an organizational culture of innovation.

The audit also can examine whether the program's procurement efforts are adequate and efficient, as well as whether the controls related to this area are functioning as intended. Further, auditors can determine whether the organization has change management approaches in place to support innovative initiatives and a method

to identify investment and funding opportunities.

Facilitating Innovation Audits

The six internal control categories are key components that fall under a government's role in a national innovation system. Internal auditors should keep these areas in mind when drafting

their risk assessments as well as the audit criteria. To that end, the evidence-based Innovation System Internal Controls Framework can offer insights that auditors can leverage throughout an engagement to ensure these programs are successful.

Perla Habchi is an internal auditor at the Government of Canada in Ottawa.

GAM
WHERE LEADERS

Great Audit
Minds



Join the most esteemed gathering

of internal audit innovators, leaders, and trailblazers from March 11-13 at the ARIA in Las Vegas, NV or virtually at 2024 GAM: Great Audit Minds (same name, new meaning of legacy and longevity).

Register by January 26, 2024 and **save \$610.**

GAM | Great Audit
Minds
WHERE LEADERS EVOLVE.



boardroom

Turning Up the Heat

The pressure is rising for boards to do better on fraud.

◆ Matt Kelly

L

ast year, a “Boardroom” article about fraud warned that fraud risk was on the rise. Eighteen

months later, only one thing has changed: The pressure for boards and auditors to mitigate fraud risk is going nowhere but up, too.

So says the U.S. Securities and Exchange Commission (SEC), which published a missive late last year urging external auditors (and by extension, internal auditors) to do better at assessing fraud risk among their clients. So says the U.S. Public Company Accounting Oversight Board (PCAOB), which put fraud at the top of its priority list for audit firm inspections in 2023 and just proposed a new standard that audit firms look more aggressively for possible compliance violations at their clients.

And so says COSO, which earlier this year updated its guidance on fraud. Its primary message: The best way for an organization to deter fraud is for that organization’s leaders to get serious about taming fraud risk.

Clearly fraud risk is having a moment. The question is how should boards and internal audit

respond to that moment, as regulators and external auditors bring more pressure to bear?

Even today, in 2023, blame COVID-19. The pandemic put all organizations through the business process blender, as everyone rushed to stand up new systems for contracting, payments, delivery, approvals, and more. The echoes of all those changes still reverberate, complicated all the more by new risks that run from inflation, to advanced cybersecurity schemes, to the environmental, social, and governance fraud known as “greenwashing.”

“COVID caused a lot of companies to move quickly,” says Cheryl Kondra, vice president, Internal Audit, at Tractor Supply Co., a retailer with \$14.2 billion in sales last year, and also a board director at Galaxy Gaming, a developer of table games for the gambling industry. “When you step back and look now, I’m not sure all those processes were completely baked at the time.”

No wonder so many voices, regulatory and otherwise, are turning up the heat.

How Boards Can Do Better

Take COSO’s recent fraud risk guidance for starters. It emphasizes the

importance of the board leading the charge for developing a strong fraud risk management program. Specifically, boards should push management to identify what the organization’s fraud risks are and how management plans to monitor those risks.

Jonathan Marks, a long-time fraud investigator and board consultant, who contributed to COSO’s recent guidance, says attention to the structure of the fraud program, and especially how fraud risks are monitored, is the missing piece.

“From a board’s perspective, establishing fraud risk governance policies, and a protocol over that, has become ultra-critical,” he says. It’s not enough for boards simply to know the company’s fraud risks; they need to assure that the organization has a program in place that works to deter would-be fraudsters.

For example, boards can start by quizzing management on what the organization’s fraud risks are, and how management chose those issues. Embezzlement and financial statement fraud are easy examples to grasp, but boards should also ask about ghost contractors, bid-rigging, kickback schemes, and a wide range of other issues. How wide a range? The Association of Certified Fraud

Examiners tracks more than 50 categories of fraud; the number of specific fraud schemes within those categories is anyone’s guess.

Next, boards need to ask management about the anti-fraud controls that are in place, and how those controls relate to the fraud risks identified. The board should then solicit internal audit’s opinion, too.

“The board should be asking the CAE, ‘What should we be looking for? How do we build a monitoring program around these key risks?’” Marks says. “That’s generally not done.”

Marks harps on monitoring so much because that, in turn, forces internal audit and management teams to develop fraud risk indicators. Pour the right data into those key risk indicators, and suddenly the red flags on fraud start rising much earlier. Or, as Marks likes to say, “Data analytics becomes the silent whistleblower.”

Anti-fraud Efforts in a More Crowded Field

Boards also need to work with another group under pressure to be more aggressive with anti-fraud oversight: the external auditor. For example, SEC chief accountant Paul Munter published a statement

“The board should be asking the CAE, ‘What should we be looking for? How do we build a monitoring program around these key risks?’ That’s generally not done.”

—Jonathan Marks, Fraud Investigator, Board Consultant



last October telling auditors to look more critically at their clients' fraud risks. Too often, he said, auditors "frame the discussion of their responsibilities related to fraud by describing what is beyond the auditor's responsibilities and what auditors are not required to do. We find this attitude ... deeply concerning."

This year, the PCAOB has warned audit firms that its top inspection priority will be how the firms approach fraud. How might audit firms respond to that pressure? By looking at issues such as the design of anti-fraud controls (including management override of controls), as well as how management and the audit committee respond to complaints about fraud or other illegal acts.

Boards and audit teams alike need to anticipate that heightened scrutiny from external auditors — including the possibility that the organization's external audit team might not always know how to approach fraud.

"No. They don't get it at all," one CAE at a public company told me. "They're just busy doing Sarbanes-Oxley compliance."

This CAE even found a small fraud at his enterprise and expressly told the audit firm, "This could be



“We’re not just focusing on accuracy and process. It has to be about fraud and what could go wrong, rather than demonstrating that everyone followed steps A, B, and C.”

—Cheryl Kondra, Vice President,
Internal Audit, Tractor Supply Co.



happening elsewhere.” Because the fraud wasn’t material, the audit firm didn’t dig further. That is exactly the sort of response that would drive Munter, at the SEC, bananas.

Still, if external auditors start raising concerns about possible frauds more often, the audit committee will need to respond to those concerns somehow. That brings us back to our earlier points about the board assuring that a fraud risk management program is in place, and internal audit assuring that the program makes sense.

Kondra wants boards to understand that each audit performed is about more than just accurate numbers. “We’re not just focusing on accuracy and process,” she says. “It has to be about fraud and what could go wrong, rather

than demonstrating that everyone followed steps A, B, and C.”

That’s what internal audit needs to bring to the board, so the board feels comfortable with fraud risk management. What about the other way around? What does the board need to bring to the organization, so that all other stakeholders are comfortable? “Governance,” Marks says, which he describes as “a waterfall system” that flows from governance to risk management to compliance.

The board first needs to understand what its fraud risks are, he

says, and then ask how the audit and compliance teams monitor and respond to those risks in a disciplined manner. “It doesn’t go any other way.”

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





Robots are helping in perilous places, so why don't they inspire human collaboration?

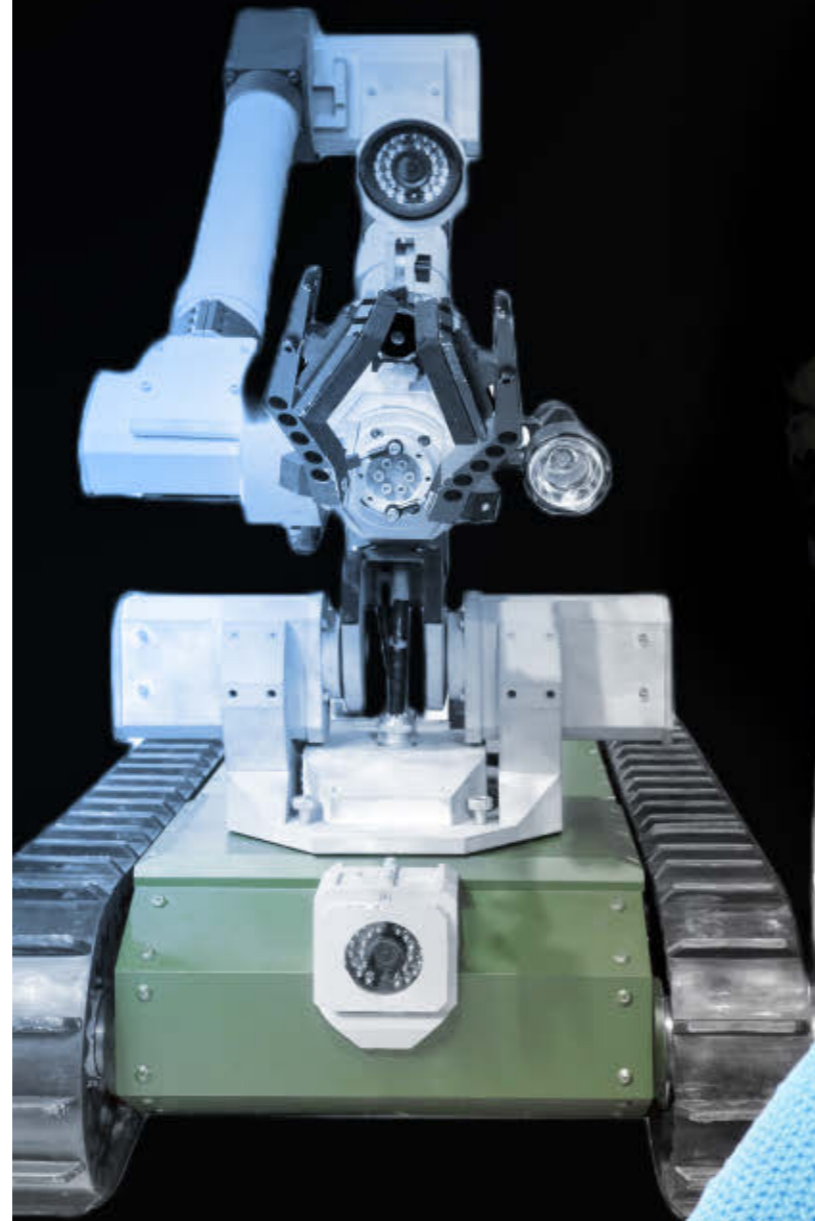
About 6:30 p.m. on April 15, 2019, the unthinkable happened: A major fire threatened to destroy one of the world's most iconic buildings, the Notre Dame Cathedral in Paris. 

The fire started in the attic and quickly spread to the roof as large flames engulfed the cathedral's spire. Fire brigades were on the scene in minutes, performing work that was both desperate and dangerous. The blaze had to be fought from inside the cathedral to avoid pushing flames further into the structure and risking a collapse. However, the roof, framed with 13th-century oak, was covered by 460 tons of lead tiles, creating a serious health hazard for firefighters as it melted.

This perilous situation was perfect for one of those battling the blaze: Colossus. A remotely controlled robot, Colossus weighs 1,100 pounds and can shoot 660 gallons of water per minute up to 800 feet. With the help of the robot, the fire was under control in three hours and only one firefighter was injured.

As robots like Colossus move into more roles once filled by people, it raises important questions about the future of human-machine

As robots like Colossus move into more roles once filled by people, it raises important questions about the future of human-machine collaboration.



collaboration: Are these robots an indisputable asset to work teams? What effect do robots have on the behavior of their human counterparts?

Szu-chi Huang, an associate professor of marketing at Stanford University in Palo Alto, Calif., recently investigated the impact of helper robots on human prosocial behavior — a key element of cooperative work (see “Connecting With the Robot Co-worker” on this page). She and Fangyuan Chen at the University of Macau in Taipa, Macao, China, co-authored a study examining whether these bots inspire people to help each other.

“We observed that disaster response robots are being used a lot by governments,” Huang says. “So we were interested to see if watching a video about them might affect how people who weren’t actually experiencing the disaster feel and behave.”

The short answer is, yes it does. And unfortunately, the effects aren’t positive. Huang’s findings raise some

Connecting With the Robot Co-worker

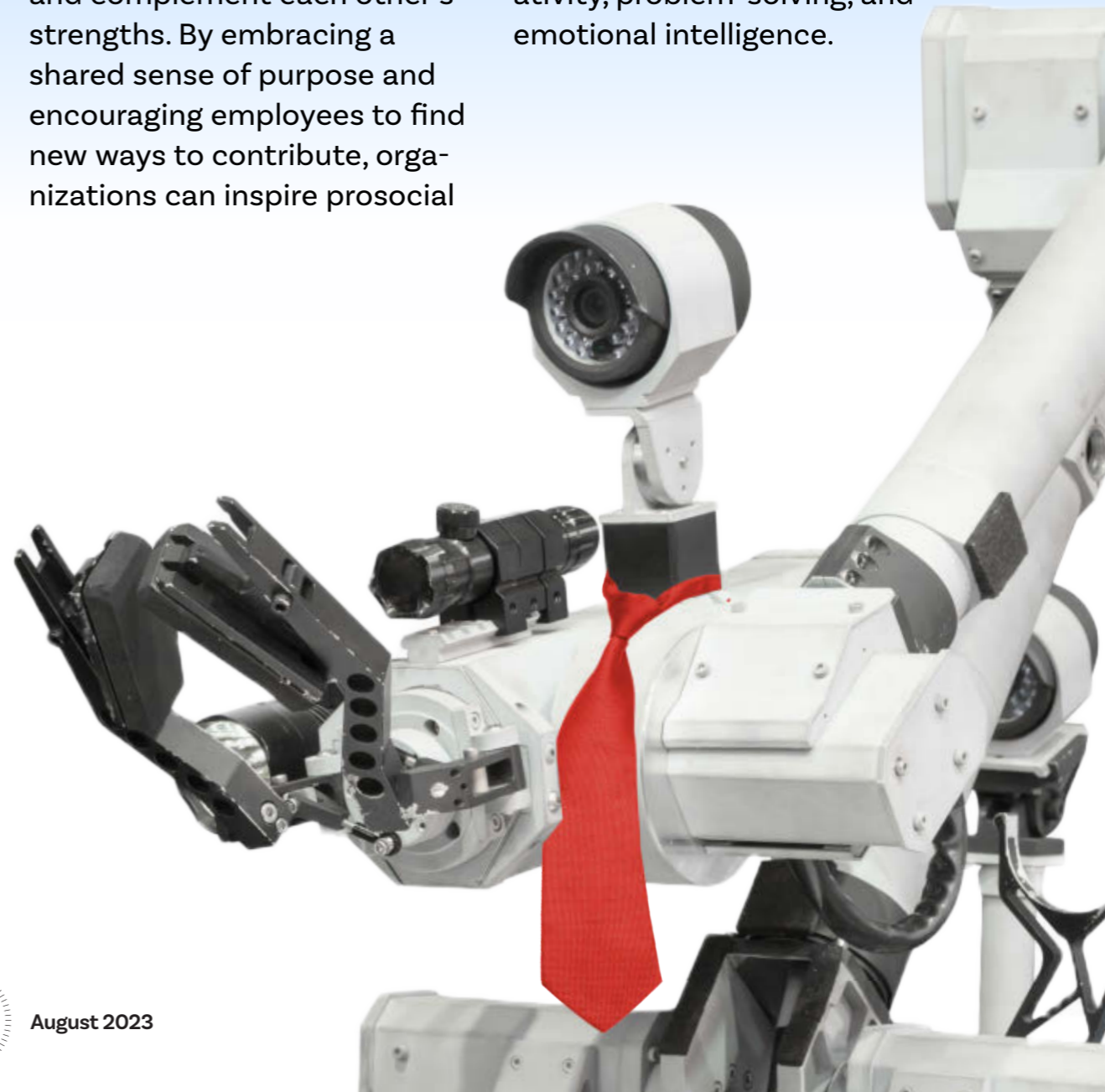
Prosocial behavior — the altruistic impulse to help others — is critical to businesses. People are inspired to work harder and help others when a teammate, leader, or even a stranger sets a positive example. This impulse is frequently summed up in the observation that soldiers don’t fight for their country, they fight for their buddy in the next foxhole. But what if the soldier in the next foxhole is a robot?

Likewise, if an employee’s warehouse co-worker is a robot that fulfills orders, is that person more or less likely to redouble his or her own efforts to get those holiday shipments out on time? The robot’s going to work at maximum efficiency no matter what. How much are employees actually “helping” — and who are they helping — by ramping up their performance?

While the presence of robots in the workplace raises questions about the impact on prosocial behavior, it also presents an

opportunity to rethink human-technology partnerships. Instead of perceiving robots as competitors, businesses can foster a more collaborative environment where people and robots work together and complement each other’s strengths. By embracing a shared sense of purpose and encouraging employees to find new ways to contribute, organizations can inspire prosocial

behavior, even in the presence of automation. Not only could this approach enhance teamwork and job satisfaction, but it may also empower employees to focus more on higher-level tasks that require human creativity, problem-solving, and emotional intelligence.



potential challenges for businesses to consider and provide insight on what to watch for as people and machines work more closely together in the years ahead.

Failure to Inspire

In one part of their research, Huang and Chen showed participants news articles about people and robots helping to disinfect hospitals during the COVID-19 pandemic — some stories highlighted the robots, while others emphasized the human workers. Then they asked the subjects to volunteer for a charitable cause or to make a donation. Those who read about the robots

were significantly less likely to contribute time or money.

Intrigued, Huang wanted to understand why this was happening. “We isolated the mechanism that drives this reaction,” she explains. “Humans are considered autonomous — we can do the same things as the robots, but we have agency over our actions. We can choose not to perform a dangerous task, but when we instead decide to put ourselves at risk, our behavior is seen as courageous and therefore more inspiring to others.”

On the other hand, helper robots are not viewed as autonomous beings — putting

themselves in harm’s way is never a choice for a robot. They are simply performing dangerous tasks because they were instructed to and were designed to withstand any hazards they might encounter. Consequently, they’re not perceived as courageous.

But what about when robots are engaged in more mundane tasks such as assisting business customers? While her research doesn’t specifically address that type of scenario, Huang says it could have significant implications for everyday commercial interactions.

“In a retail setting, if a robot is seen working with

a customer who needs help, for example, that might not be as inspiring for those visiting the store compared to seeing a human offer assistance,” she says. That lack of inspiration could negatively impact the way consumers perceive and engage with the company’s brand.

Human interaction with other advanced technologies, such as generative artificial intelligence (AI) tools, could have the same effect. Huang says neglecting to manage these tools carefully could make employees or customers less willing to help each other.

For example, when a team member is struggling

with a new initiative, his or her colleagues — knowing that AI has contributed to the effort — may not be as inclined to pitch in. “The impact on our prosocial behavior — and humanity as a whole — could be costly,” she warns.

Autonomous Allies

While Huang’s research identifies potential problems, it also points to some possible solutions. It’s critical to frame communications around the use of AI and robots appropriately, she says.

In many organizations that use robots, they are working alongside humans. When deployed in a warehouse setting, for example, the machines are often called co-bots. The human and robot function as a team, collaborating to solve problems. By emphasizing the human-machine partnership in that situation, the robot’s actions may be seen as more autonomous and more inspiring. Emphasizing the vulnerability of the robots — they’re often



“If a robot is seen working with a customer who needs help, for example, that might not be as inspiring for those visiting the store compared to seeing a human offer assistance.”

—Szu-chi Huang, Associate Professor of Marketing, Stanford University

used in situations that can literally destroy them — can also be leveraged to imbue them with more human qualities such as courage that would inspire people.

Emotional Connections

Huang is working on a study to better understand how humans relate to robots emotionally. “We’re now looking at substitution — how employees feel if part of their work can be done by robots and machines,” she explains.

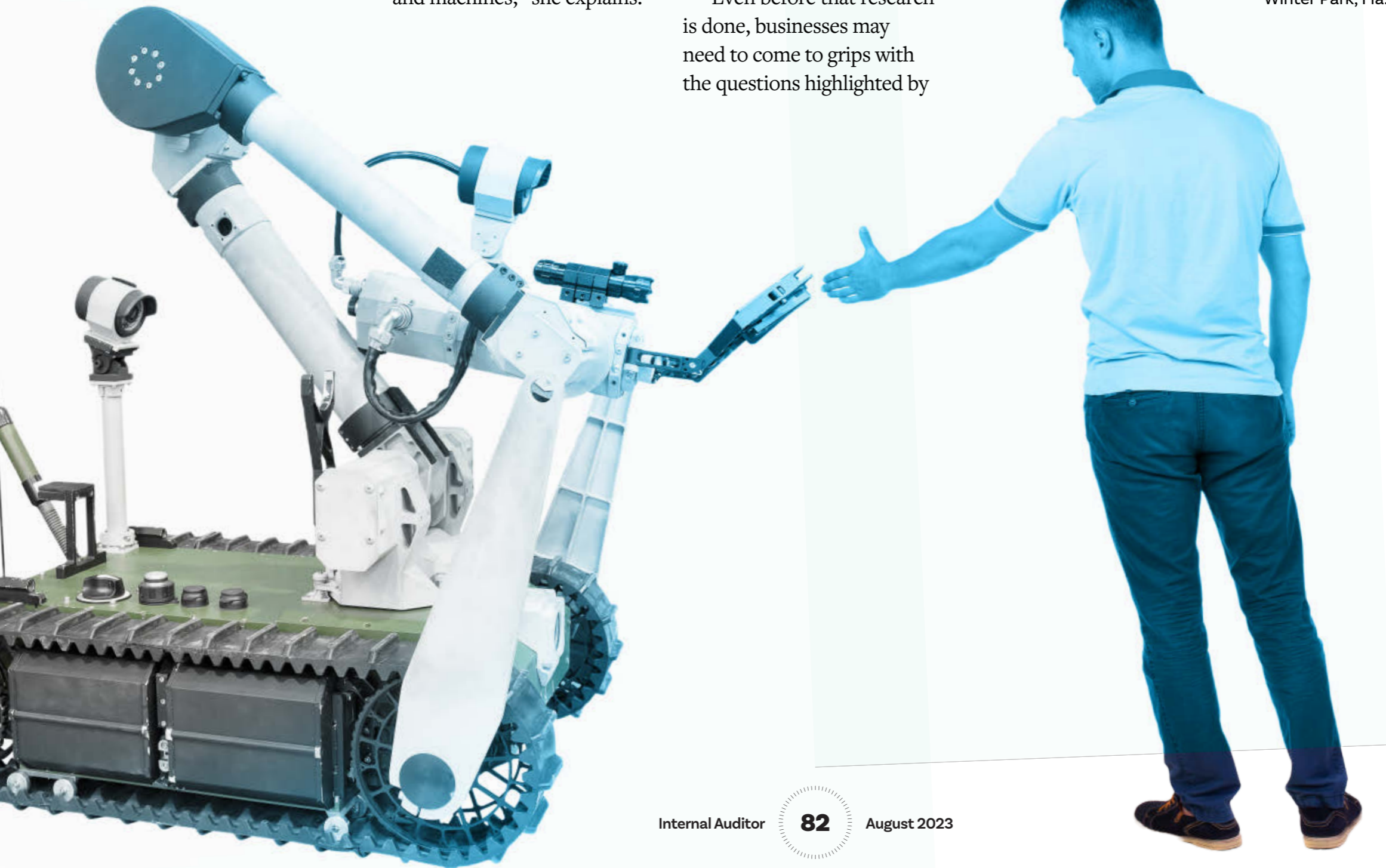
She also is looking at applying human features to robots. “What if we give them some facial features — does that make people interact differently with them?” she says. “And how does that change our perception of the robots?”

Even before that research is done, businesses may need to come to grips with the questions highlighted by

Huang’s existing studies. Integrating robots and AI technology into organizations in a way that inspires prosocial

behavior is rife with problems, but also with potential. Those who do it successfully could reap substantial benefits not just to morale, but also to the bottom line.

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



Inspiring.
Evolving.
Innovating.
Your World.



Elevating internal audit quality around the world.

IIA Quality Services provides vast expertise, resources, and services to conduct a cost-effective and expert external assessment of any internal audit function, anywhere – taking further, farther.

A natural choice. theiia.org/Quality

2023-6163



viewpoints

Putting Automation to Work

Internal audit needs to be strategic in its approach to automating controls.



Richard Kloch, Jr.
Partner, Crowe

How is automation changing the way organizations do business?

For years organizations have been using the phrase, “do more with less.” Automation allows them to put this phrase into action. It can reduce the time employees spend on manual tasks, allowing them to focus on critical strategies that historically have been ignored.

Applying automation allows the internal audit function to take a continuous auditing approach and test an entire population in a fraction of the time, and with fewer resources. The results provide valuable data and insights that allow management to make better,

faster decisions related to risks and strategy.

What tasks are being automated?

Organizations initially developed automation to enhance the customer experience and help expedite common first-line processes. With these successes, more companies are now allocating funding and resources to internal audit.

To understand where automation should be applied, the function should focus on how much time and effort is saved through its use. This will allow it to rank which areas should be addressed first to provide the biggest return on investment. To date, that has been areas with

highly repeatable controls and processes.

What are some challenges in adopting automation?

Many organizations' controls are highly manual, which makes it difficult to quickly adopt automation. Organizations need to be strategic about the areas they want to automate. Internal auditors can help because they come across a wide range of issues and problems on the job. Once their understanding is paired with a forward-thinking approach, one that aligns the audit plan with an organization's overarching objectives, it should be much easier to decide which departments and processes would most benefit from automation.

Another pain point is around skills and training. While it may be easy to go outside of the organization to obtain the skills to develop and implement

automation, who is going to be responsible for overseeing these changes in the long term?

Finding and retaining or training employees can be time-consuming and costly, but it's an important investment to make. When companies introduce automation, it's critical to have employees who not only oversee the process but can use data to make smarter decisions moving forward.

Another challenge relates to funding and internal audit's

reputation in adding value. Internal audit is often viewed as a cost center and not as a strategic function, and therefore automation funding may end up elsewhere. However, leaders who view internal audit strategically and make the right investments will have a competitive advantage over their peers and will reap the enormous benefits automation presents for expanding risk coverage and driving enterprise value.

While it may be easy to go outside of the organization to obtain the skills to develop and implement automation, who is going to be responsible for overseeing these changes in the long term?



Miles Hitchcock
Director of Product Marketing,
Diligent

What are the biggest risks to integrating automation?

While automation offers many advantages, there are some potential risks that organizations should consider. For example, automated systems are sometimes prone to technical failures, such as software glitches or hardware malfunctions. These failures can disrupt operations, cause delays and result in financial losses. However, having robust backup systems and contingency plans in place can mitigate this particular risk.

Another risk involves data security and privacy. Automation naturally requires the collection and processing of large amounts

of data. Protecting this data from unauthorized access, breaches, or misuse is of paramount importance. Using a best-in-class automation system that complies with industry-leading security standards and authorizes only certain users to access the data minimizes this risk.

What are the biggest benefits of automation?

With growing responsibility for risk oversight, especially in complex areas such as cybersecurity and ESG, today's internal audit teams are busier than ever. Automation can replace time-consuming and repetitive processes with more efficient workflows that reduce

costs and eliminate the need for additional headcount.

There are only so many controls that a single internal auditor can check manually, and the assessments typically reflect a single moment in time. But when automation is appropriately integrated, it can provide continuous, real-time insights and constant assurance that controls are working as they should, reducing the risk of a compliance breach. This continuous monitoring also scales easily: As audit work increases with organizational growth, automation scales with those needs.

Moreover, automation reduces the risk of human error — which is never fully avoidable when using manual processes. All auditors strive to reduce human error, of course, but error reduction is particularly important in industries

where accuracy is crucial, such as manufacturing, finance, and healthcare.

What are some considerations for auditors using automation?

Before they begin using automation, auditors should have a clear understanding of the processes they want to implement, as well as their underlying documentation. This includes system specifications, policies, and procedures.

Keeping the aforementioned risks in mind, audit teams should identify vulnerabilities and potential impacts

on objectives, focusing on areas where automation has the highest risk exposure. Making sure that the automated systems adhere to relevant regulatory requirements, industry standards, and internal governance frameworks is also key, especially where data protection, privacy, and cybersecurity are concerned. Additionally, auditors should ensure the data used in automated processes is reliable and complete. The same goes for any controls implemented within automated systems. Audit teams should thoroughly

review access controls, segregation of duties, error handling mechanisms, and monitoring and logging practices.

Finally, keep in mind that while automated processes are designed to perform specific tasks efficiently, they may lack the flexibility and adaptability of human workers. Unforeseen circumstances or changes in requirements may call for human intervention or system reconfiguration.

Audit analytics solutions that offer scalability and can adapt to changing needs may address these concerns and potential risks.

Keep in mind that automated processes may lack the flexibility and adaptability of human workers.



IMMERSE YOURSELF

In An Executive Experience.

September 25-28, 2023
Four days to amaze and immerse.

theiia.org/VisionU

Vision University





IAm

Hansha Khoosy

It was through my job that I discovered a love of travel. I look forward to taking trips during my time off from work and tend to dedicate free time to family vacations.

I've been fortunate to have traveled the world and visited 21 countries so far. I'm always captivated by the unique atmosphere found in Latin American countries – from the vibrant energy of Rio de Janeiro, to the rich and diverse flavors of Colombian cuisine, to the fascinating architecture of Buenos Aires.

Whether it's tasting exotic dishes such as tamales in Mexico and delicious Trdelnik in Prague, immersing in local traditions, or simply marveling at iconic landmarks, every moment spent on the road has been filled with excitement and wonder.

Internal audit gave me wings to fly. Although I had a predetermined path to work for a Big Four firm and become a finance professional, after discovering internal audit, I haven't looked back.

Because my daughter is a pandemic baby, my aim is to begin sharing family adventures and my love for traveling with her very soon.

stats

CIA

Senior Manager,
Internal Audit
IQ-EQ

Port Louis,
Mauritius