RECRUITING **GEN Z**
A succession plan for the profession

TAKE **ACTION**
The climate change journey

LET'S GET **PERSONAL**
The relationship side of auditing

internal auditor

FEBRUARY 2022
A PUBLICATION OF THE IIA

A Brave New World

Auditors see uncertainty and opportunity in 2022.

The Institute of
Internal Auditors

Elevating Impact

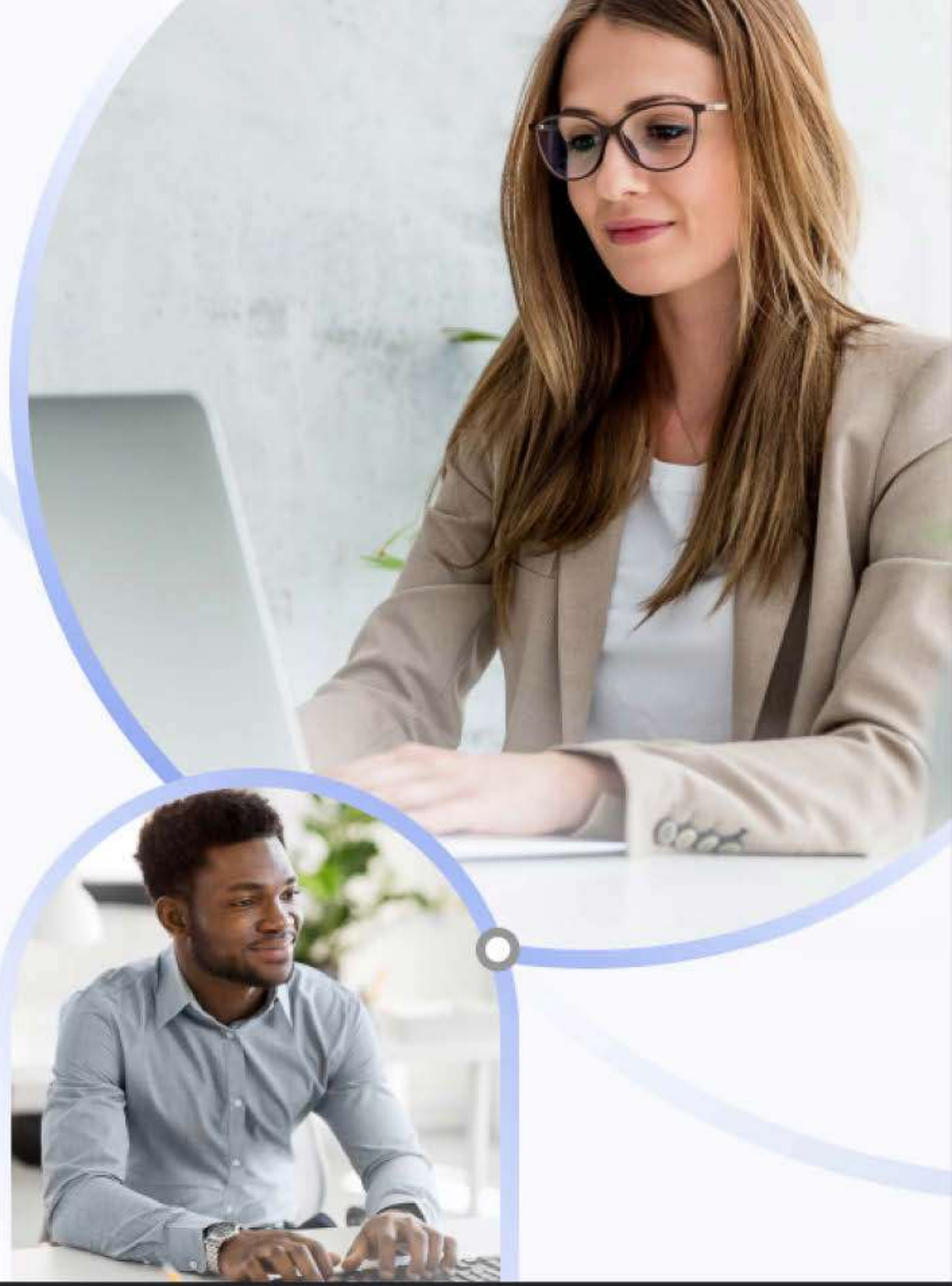
The IIA empowers internal auditors to foresee potential risks that drive organizational success and enhance value. Elevating impact at every level, the world over, we are The IIA.

Membership | Standards | Certifications | Learning ***www.theiia.org***

Connect Risk. Connect Your Teams.

THE MODERN CONNECTED RISK PLATFORM

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



TOP-RATED AUDIT SOFTWARE ON

Gartner peerinsights

g2.com

Capterra

REQUEST A DEMO AT AUDITBOARD.COM/DEMO

AUDITBOARD

Empowering Leaders,

Influencing Change.

GAM

WHERE LEADERS EVOLVE.

GAM remains on the cutting edge of top-tier events for top-level internal audit leaders. Get ready to immerse yourself in an interactive experience like no other and engage with industry leaders, like-minded peers, and forward-thinking presenters and exhibitors.

MARCH 14–16, 2022 | ARIA RESORT & CASINO | LAS VEGAS & VIRTUAL

The evolution starts here www.theiia.org/GAM

The Institute of **Internal Auditors**

Elevating Impact

2021-3858

contents

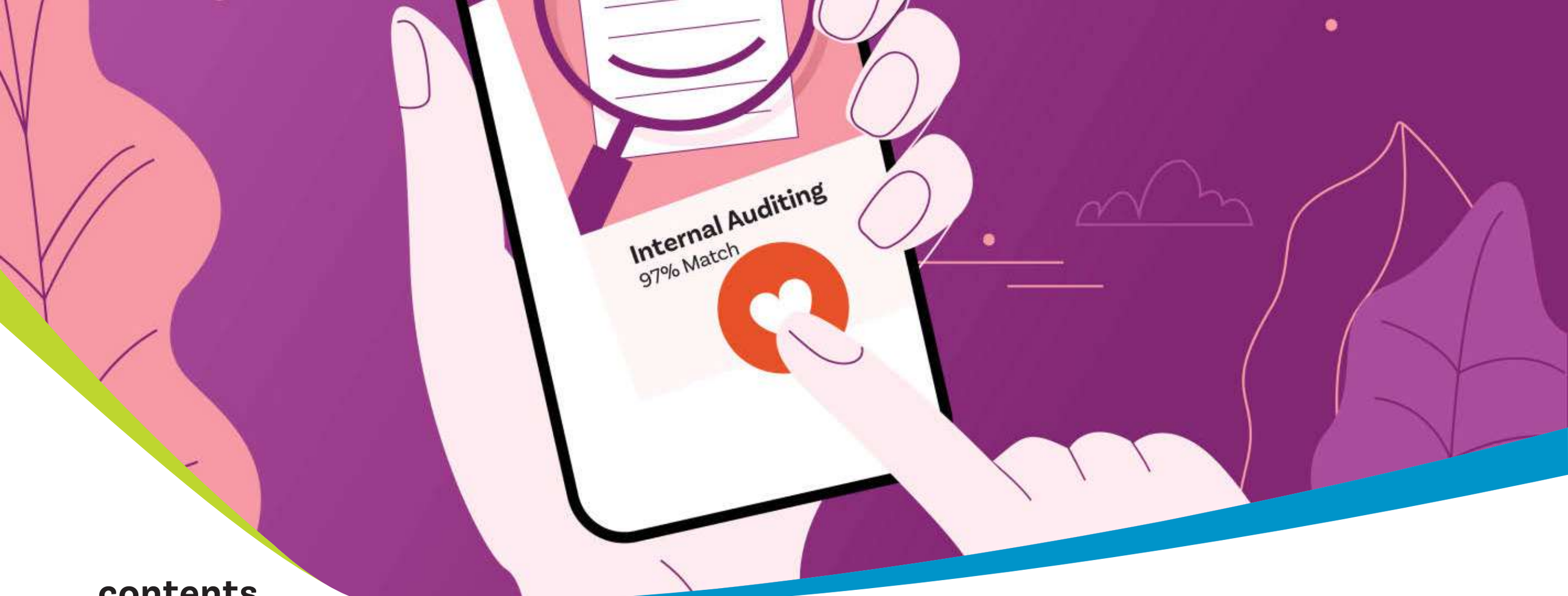
Featuring

29

A Brave New World

As the world approaches the second anniversary of the COVID-19 pandemic, organizations continue to grapple with several major risks that the crisis either created or exacerbated. With many offices reopening, organizations and internal auditors are returning to a very different business environment marked by new operational, workplace, technology, and social risks.

Neil Hodge **Douglas Tocco**

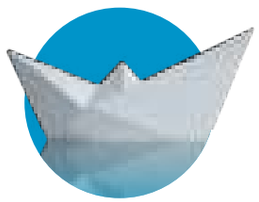


contents

Featuring

contents

Practices



contents

Insights

> CERTIFICATION

Certified *for Success.*

Success is measured by the impact you make.

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

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

CIA® Certified Internal Auditor®

ceo message

Finding Opportunity in Adversity

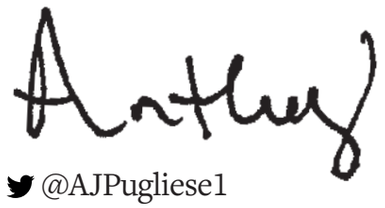
remember the early days of 2020, which feels like a lifetime ago, first hearing the name that would turn our world upside down: COVID-19. None of us could have imagined that we'd still be battling the pandemic two years later, let alone predict the ways it would change nearly every aspect of business and our daily lives. From supply chain disruptions to homeschooling, remote working to normalizing mental health discussions, our world has changed and there's no going back. That's not necessarily a bad thing.

To be sure, the pandemic disrupted life on a scale of historic proportions. But for every disruption, we've discovered a new opportunity. You'd be hard-pressed to find parents who enjoyed home schooling their children while balancing their own jobs, but remote learning and working are now more widely accepted, and that flexibility is undoubtedly a good thing. Yes, business was slowly trending more virtual/remote before the pandemic, but necessity accelerated these and other trends.

COVID-19 forced industries to operate differently. Businesses have adopted new processes and technologies to improve efficiency and manage the challenges of new safety protocols and a dispersed workforce. The pandemic also pushed internal audit functions to accelerate adoption of technologies they may have been considering for years. Drones, for example, are being used for inventory observations, enabling auditors to be more efficient and making their job safer by completing dangerous tasks. Other types of robots and artificial intelligence systems are handling data-heavy computations that free up auditors to focus on higher value areas that only a human can address. This technology gives auditors new ways to provide assurance that critical functions are being maintained and helps address tasks made more difficult by the pandemic. Now we must ask how we can leverage these lessons to get in front of other technology developments.

And as technology evolves, there's an accompanying need to create standardized processes to ensure quality, consistency, and privacy with each new advancement. Our profession is at the heart of this transformation — the independent internal audit function is uniquely positioned to provide objective assurance that organizations are adopting new technologies efficiently and responsibly.

As the last two years demonstrate, we can't predict what comes next, but our pandemic-honed agility will serve us well. As you read this issue, consider how we can apply the lessons we've learned over the last two years to tackle the challenges ahead and seize the opportunities that await. In fact, we're seizing opportunities right here with a new digital design of our magazine. This redesign reflects the world's more digital approach to business and will bring our content to life in new ways. We're excited to share this new experience and the great content to come this year.



@AJPugliese1

internal auditor

February 2022

Published by

The Institute of Internal Auditors

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

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

editor's note

A Brave New Look!

Notice anything different? We are beyond excited to share with you a completely redesigned *Internal Auditor* digital magazine and InternalAuditor.org website.

The last time we redesigned the magazine was in 2012. In 2022, we're unveiling it in conjunction with the launch of The IIA's new, digitally transformed website. What's different about this redesign? Everything! It's a digital world, and we've redesigned InternalAuditor.org and the magazine with that in mind.

In recreating the digital magazine, we brought on a new designer, Em Agency. We threw out all the rules of print design and instead approached the job with a digital-first mindset, actually turning the magazine on its side. This magazine is designed for the screen — not the page. With this digital design, a two-page spread becomes a single, full-screen and there's no need to squeeze as much text as possible onto each screen. We let the design breathe and flow. This innovative digital publication features a bold design; larger, more easily readable fonts; and a variety of other digital-first offerings that enhance the reader's experience.

With this issue, we've also refreshed our content and are introducing two new departments: "The Big Idea" (page 68), in which we explore new and innovative happenings in internal auditing and the business world, and "IAm" (page 76), in which we put a face to The IIA member. Our members hail from around the globe. They are diverse in every way, and we want to share their stories with you.

The redesigned InternalAuditor.org offers the same exciting new features and functionality as The IIA's new site (www.theiia.org). Using similar design aesthetics, the site boasts a brighter, more dynamic, and more user-friendly look and feel.

As you rediscover your *Internal Auditor* magazine and InternalAuditor.org, make sure you experience all that the platform has to offer — from the English and Spanish digital editions, to web exclusives, to blogs, to videos, and soon podcasts — we're providing our readers more quality, informative digital content than ever.

I hope you find *Internal Auditor*'s digital transformation as exciting as we do. I'd love to hear your feedback. Contact me on LinkedIn (Anne Fobear Millage) or Twitter and let me know what you think.

Anne

@AMillage

update

Fighting the Fatigue Factor

IIA report shows fewer companies earn high grade for governance.

Among U.S. publicly traded companies, 2021 proved to be one of the greatest tests of corporate governance in recent years, according to The IIA's latest American Corporate Governance Index (ACGI). Nearly across the board, governance improvements retreated, notes the survey produced in collaboration with The University of Tennessee's Neel Corporate Governance Center.

For example, the number of companies earning "A" grades in governance dropped from 19% in 2020 to 14% in 2021. There also were notable declines in improvements to employee governance measures, such as providing adequate training and compensating in a way that promotes ethical decisions.

The annual ACGI report gives publicly held U.S. companies a score based on the strengths, weaknesses, and effectiveness of their governance practices and policies for the previous year. As in 2020, companies overall earned a B- grade, but the average score dropped from 82 to 81.

The report shows that the many effects associated with the ongoing global pandemic have led to "fatigue" regarding governance improvements. "Although a decline of one point seems small, it's out of alignment with the increased scrutiny on companies to improve their governance as they face continued market and regulatory pressures," says Anthony Pugliese, president and CEO of The IIA.

One area where companies are facing regulatory, shareholder, and stakeholder pressure is environmental, social, and governance (ESG) reporting. Survey participants report a growing focus on these issues, but fewer than one in three CAEs rate ESG-related information being used internally or presented externally as "very good" or "excellent." **—L. Wamsley**

37%

REDUCTION OF IN-PERSON WORKDAYS PER WEEK

Gallup analysts predict a significant reduction of in-person days worked per week among U.S. employees for 2022 based on workers' preferences for remote work.

SOURCE: GALLUP, THE CHAIRMAN'S BLOG

The Path to Net-zero

Major companies across regions and sectors are setting net-zero emissions targets.

80%
of 180 companies surveyed are developing a net-zero emissions target plan.

26
of the 30 largest U.S. utility companies have a net-zero target.

21
of the 30 largest U.S. and European health-care companies have a net-zero target.

SOURCE: S&P GLOBAL MARKET INTELLIGENCE

Twin Threats Driving Cybercrime

Ransomware, network access sales are up.

Ransomware is evolving and becoming more sophisticated, making it the No. 1 cyber threat worldwide, according to the Hi-tech Crime Trends Report from global cybersecurity services provider Group-IB, based in Singapore.

In the first 11 months of 2021, more than 60% of all incidents investigated by Group-IB were ransomware-related. Paramount to the success of these bad actors is the use of double extortion tactics, which involves a threat to publish company data as well as steal it, to increase incentives for victims to pay ransoms. Triple extortion methods that extend ransom demands to clients or suppliers are also becoming increasingly common.

In addition to the focus on ransomware, the report has four other primary areas of focus: the sale of access to corporate networks, cyberwarfare, threats to the financial sector, and phishing and scams.

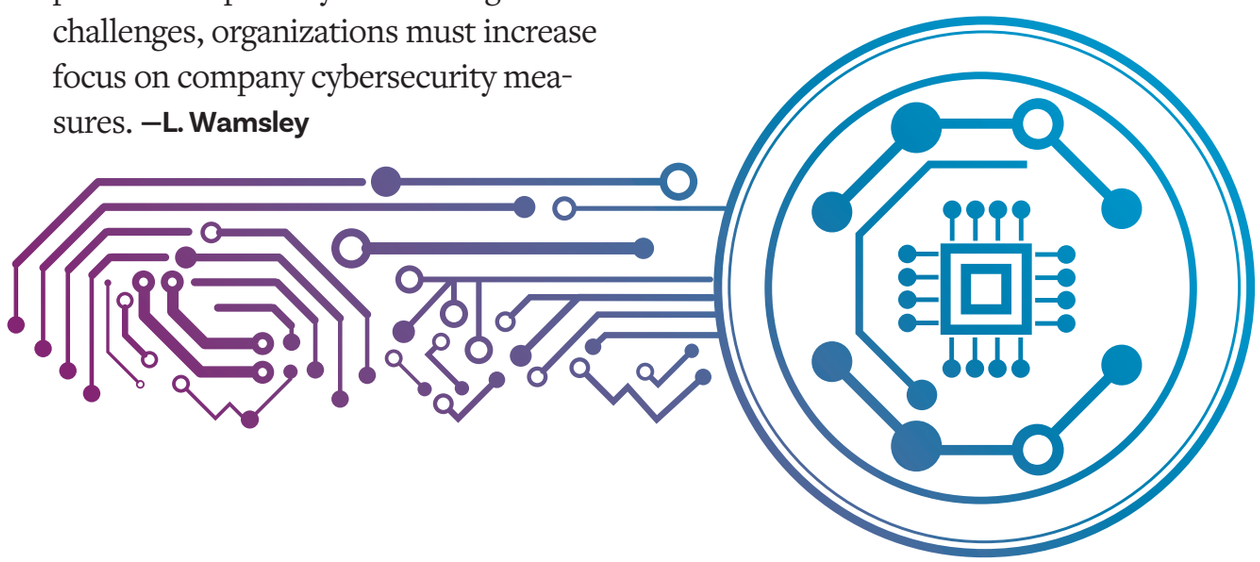
Among these areas of focus are a few particular causes for concern. For example, the report finds a dramatic increase in the number of offers by cybercriminal brokers to sell access to compromised corporate networks. This segment has a relatively low entry barrier, and combined with widely available tools for conducting attacks and generally poor corporate cyber-risk management, is ripe for growth. Between the first half of 2019 and the second half of 2020, the Group-IB Threat Intelligence team detected only 86 active brokers; between the second half of 2020 and the first half of 2021, this number increased to 262.

The rise in cybercriminal brokers combined with the increase in sophistication of ransomware operators has resulted in a staggering 935% increase in incidents where company data was made public. Group-IB says that facing such challenges, organizations must increase focus on company cybersecurity measures. **—L. Wamsley**

51%

OF ORGANIZATIONS
have faced one or more third-party risk incidents since the start of the pandemic. **13%** were high-impact incidents that severely affected financial performance, customer service, and regulatory compliance.

SOURCE: DELOITTE, INTERNAL AUDIT: RISKS AND OPPORTUNITIES FOR 2022



ASK AN EXPERT

ESG Reporting at Light Speed

What's happening with environmental, social, and governance (ESG) disclosure that auditors need to be watching?

The formation of the International Sustainability Standards Board (ISSB) announced at COP26 last November was the culmination of at least a decade of effort to push for a uniform global standard for sustainability reporting. The ISSB was formed simultaneously with the merger of the Sustainability Accounting Standards Board (SASB) and the International Integrated Reporting Council (IIRC) into the IFRS Foundation. The creation of the ISSB has happened at lightning speed compared to what we saw on the financial reporting side of the equation. It's anticipated this speed and agility will continue. We've had predictions that a first draft of a set of global sustainability reporting standards could come out as early as the first quarter of 2022, or at least by the third quarter. That's very fast, but we've been talking for more than a decade about the impact of ESG measures on a company's true value — and the idea that most of that value is found off the balance sheet in other nonfinancial factors.

"It's incredible to note that throughout the period leading up to the formation of the ISSB, internal audit's voice was really missing. The profession has an opportunity now to strengthen and make its voice louder."

What should internal auditors do to get ready for changes to nonfinancial reporting?

Venturing into the ESG disclosure reporting space doesn't require internal auditors to learn new skills. It's still about the fundamentals of having effective controls, continuous monitoring, and all of those other things they would do with financial information applied to a new data set. Internal auditors should be following relevant announcements from the ISSB, as well as the U.S. Securities and Exchange Commission and its equivalents around the world, and take the time to understand how their organization is going to be impacted by the coming changes. CAEs should refer to the Three Lines Model so they can have that conversation on what their role needs to be. Boards are not always sure how to leverage internal audit, and the CAE needs to inform the audit committee that it needs strong, objective assurance over ESG information — investors will make decisions on what comes out in these reports. It's incredible to note that throughout the period leading up to the formation of the ISSB, internal audit's voice was really missing. The profession has an opportunity now to strengthen and make its voice louder.

Brad J. Monterio, is the executive vice president for member competency and learning at The IIA and a member of the IIRC as voting representative for the Institute of Management Accountants.

MEMBERSHIP

Unlocking the Potential *Within*

When you join The IIA, you begin a personalized journey of knowing why and navigating how, no matter what … to unlock the potential within.

Student | Member | Certified | Executive

Find your in www.theiia.org/Membership

The Institute of **Internal Auditors**

Elevating Impact

basics

Data-enabled Internal Auditing

Many internal audit functions have yet to take full advantage of all of the opportunities that AI and data analytics present.

Muhammad Hassan Rizvi

With continuous expansion of technologies such as artificial intelligence (AI), cloud computing, and big data, organizations can now store and process more data than ever, making it easier for them to drive business strategies and decisions based on data analysis insights. With growing technology use in business decision-making and its impact on the global business paradigm, many internal audit departments have yet to adopt all of the opportunities that AI and data analytics offer.

Benefits

Data-enabled internal auditing can be a driver of change for organizations and can provide a performance- and risk-based outlook to audit engagements. Businesses can benefit from data-enabled internal auditing in a variety of ways.

Performance Reporting Internal audit can provide timely performance reporting to the audit committee and management by mapping performance against key risk indicators (KRIs) and critical success factors. This can enable business leaders to begin remediation of risks that could have a significant impact on achieving organizational objectives.

Fraud Prevention and Detection Internal auditors can proactively identify fraud instances by using red flags embedded in the internal control systems. The system will raise red flags if it identifies an instance, not fraud, itself. For example, if a parameter has been embedded in the control system that the invoices are raised against, like the same supplier for the same type of materials within the same month, then the system should generate an alert.

Continuous Monitoring Data-driven audits can focus on defining the threshold that would trigger a fraud alert, such as by number, amount, category, and frequency of transaction. An auditor can follow through on such alerts to identify a potential breach of authority, policy, or procedures. This capability

Data-enabled internal auditing can be a driver of change and can provide a risk- and performance-based outlook to audit engagements.

can enable businesses to monitor control activity on a more automated basis.

Enhanced Risk Assessment and Risk Coverage Risk assessment may be improved by linking risk analysis with the KRI database, risk loss reporting, and governance risk compliance dashboards. Linking risk analysis enables an internal auditor to identify processes with high-risk impact and likelihood rather than by merely using judgment. Moreover, it may improve audit coverage by:

- Identifying the correct audit to be performed.
- Increasing the number of audits per year.
- Decreasing the time required to cycle through the audit universe.
- Increasing the frequency of audits in key risk areas.
- Increasing the scope of specific audits.

Audit Effectiveness Adopting the data analytics approach can build critical data analytics capabilities within the internal audit department. For example, analytics can make the function more effective at detecting risk and data anomalies, as well as identifying performance improvement opportunities across the organization. Moreover, by enabling auditors to select high-risk samples, this approach can decrease the time auditors spend on testing and the amount of disruption to audit clients.

> Analytics can enable dynamic audit planning using a ***technology-enabled, quantitatively enhanced, continuous risk assessment process.***

Risk-based Internal Audits Using data analytics to detect anomalies can help internal auditors identify high-risk areas within the audit universe and develop audit themes for selecting end-to-end, high-risk processes for audits.

Developing dashboards and analytic reporting on metrics such as KRIs and key performance indicators (KPIs) within each operating area of the organization can help auditors leverage continuous auditing. It also can provide a platform for more robust and continuous risk assessment processes for audit planning.

Moreover, internal audit can link to the organization's strategic objectives by developing audit themes derived from the results of periodic KRI assessments.

The Audit Process

Data and analytics can be embedded in several phases of the internal audit cycle. For example, auditors can use business intelligence tools for pre-fieldwork scoping such as data discovery. Analytics can enable dynamic audit planning using a technology-enabled, quantitatively enhanced, continuous risk assessment process. Auditors can also use analytics for specific tactical efforts such as proactive fraud protection. This data-enabled internal audit approach may consist of several steps.

Analyze the Audit Universe Internal auditors should analyze the audit universe to determine and select audits that can benefit from the use of data analytics based on factors such as:

- ***Availability of data.*** Check if sufficient data is available to analyze the area under review, and if business technology is available to capture the data source.
- ***Reliability of data.*** Evaluate if the data available is obtained through a reliable source and is consistent.
- ***Risk analysis.*** Based on the risk assessment performed, an auditor will evaluate if the area under consideration is assessed as high risk. The higher the risk assessment,

the higher the priority for the process to be selected.

- ***Complexity.*** Data complexity is based on the number of sources the data is derived from and the time required to obtain it.
- ***Frequency.*** This refers to the number of times the audit is required to be performed during an annual audit period.

Develop the High-level Scope
Internal auditors should review the process risk points of the area under review to determine the KPIs, KRIs, trends, or anomalies that would make a difference in the scope of the audit.

Execute the Audit The execution step begins with data extraction. Internal audit can obtain data sets through management information systems reporting, knowledge management systems, and customized user reports from the available system capabilities, which are identified during the phase of analyzing the audit universe. Once the data is received, auditors should extract relevant data points from the source system, transfer it into a database format, and load it into an analytics engine.

Next, auditors should analyze the data to identify potential issues, trends, and anomalies. They can use an analytics engine to perform advanced analysis, including rule-based scripts, descriptive models, or predictive models. This may require help from a specialist with advanced technical training and relevant experience.

Analytics should be integrated into an audit program to meet objectives. Auditors should design and test this program using data analytics-based audit procedures that achieve audit objectives. For example, a vendor management audit might include:

- Activity — vendor data master maintenance.
- Process risk — operational inefficiencies because of ineffective vendor master data management.
- Traditional procedure — verification that purchasing management periodically reviews and actively corrects vendor master data for any inaccuracies or incomplete data.
- Data-enabled audit procedure that generate statistics for each field in critical datasets, including reviewing metrics for in-scope data elements.

Once audit procedures are complete, internal audit should examine results and develop insights. Auditors should perform additional fieldwork to validate that the analysis was performed correctly and identify the trends, anomalies, or issues that should be reported. They should use a visualization tool to validate the results of the analysis.

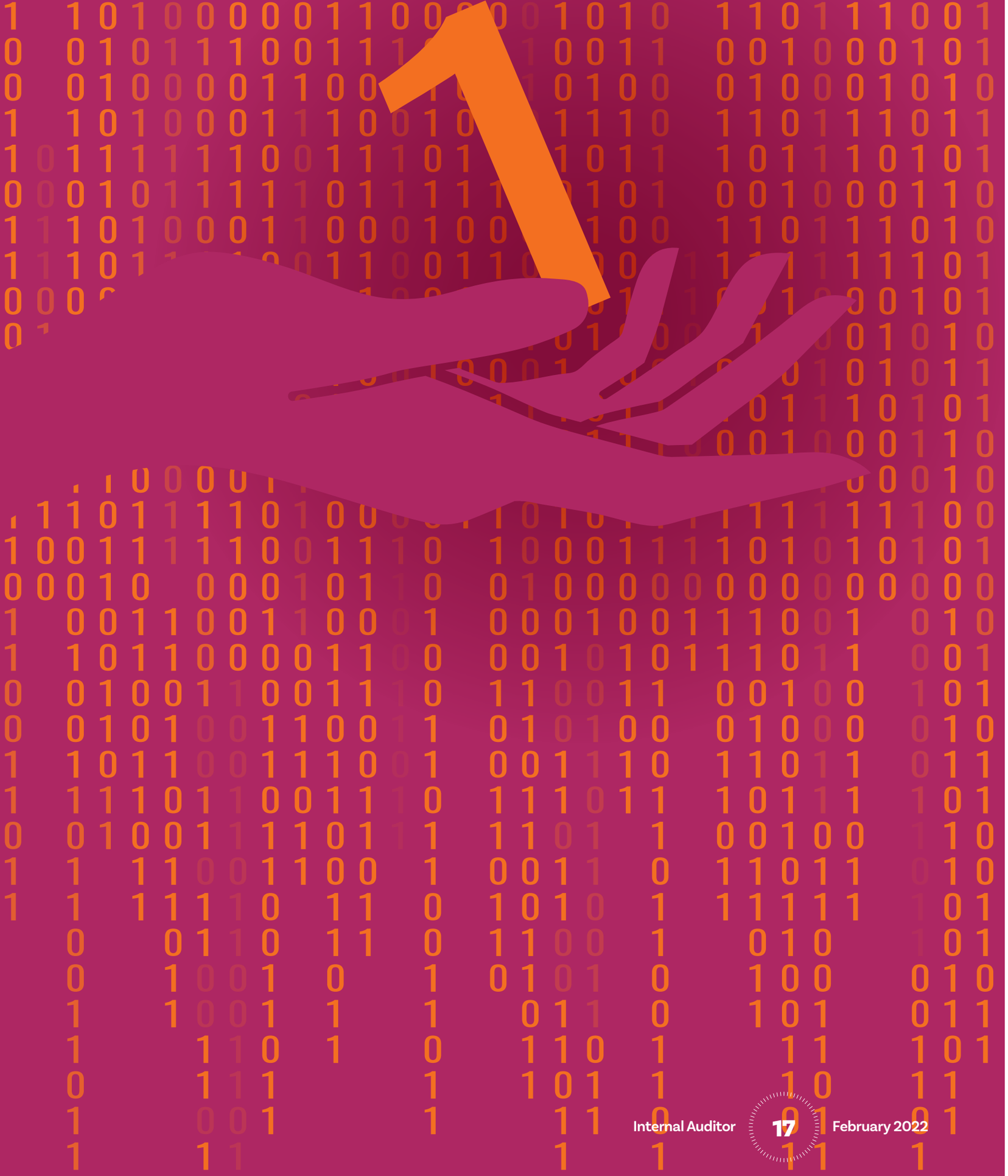
Auditors should perform additional fieldwork to validate that the analysis was performed correctly *and identify the trends, anomalies, or issues that should be reported.*

Report the Findings Once the audit is completed, internal auditors should report the results using a visualization tool that allows for enhanced reporting through data connection, extraction, and analysis linked with KPIs and KRIs. A standard audit report that can be shared with management also may be used. In addition, an auditor may design and establish reporting mechanisms, data-analytics dashboards, balanced scorecards, and alerts.

The Journey

Implementing the data-enabled internal audit approach can be a long journey. To begin, the CAE can design a pilot project and perform one engagement using this approach and can further refine the internal audit strategy.

Muhammad Hassan Rizvi is a senior consultant at Grant Thornton UAE in Dubai.



tech

Targeting Fraud With Data Analytics

Audit tools can help practitioners enhance fraud risk assessments and uncover common schemes.

Alisanne Gilmore Allen

Data analytics is one of the most effective anti-fraud controls. According to the Association of Certified Fraud Examiners 2020 Report to the Nations, organizations that use predictive data analytics discover frauds much sooner than organizations that don't monitor data for signs of fraud, and those frauds were 33% less costly.

One reason for these findings is that data analytics can help internal audit perform fraud risk

assessments more effectively. These assessments may involve identifying a common set of fraud risks — related-party relationships, fraudulent vendors, and payroll schemes — and mapping them to internal controls designed to mitigate them.

Deeper dives and additional analytics may lead internal auditors to identify potential fraud risks that may not be obvious from an initial glance. Some frauds may be difficult for practitioners to detect, given the sophistication of the crimes. However, with the appropriate technical skills and use of IT audit tools — and the imagination of a fraudster — internal auditors can increase the likelihood of identifying issues that warrant further investigation.

Deeper dives and additional analytics may lead internal auditors to identify potential fraud risks *that may not be obvious from an initial glance.*

Related-party Relationships

Many organizations have policies that prevent employees from engaging with related-party vendors without appropriate disclosure. Such policies would not allow an employee to hire his or her spouse's organization to provide services without a competitive bid, for example. In such an arrangement, the employee may benefit from the spouse's engagement, but the organization may not get value for the services.

Using analytics, auditors can check for relationships that should be investigated by comparing vendor addresses to employee addresses, or vendor phone numbers to employee phone numbers. Are these relationships appropriate? Were they known to the organization? Were they disclosed to leadership and in the organization's financial statements?

While these relationships may not be illegal, internal audit should confirm that management is aware of them by determining how many have been disclosed to the organization's CFO or general counsel. Also, auditors should verify that these vendors were subject to vendor-selection processes such as getting quotes from multiple bidders and providing the best prices and value to the organization.

Fraudulent Vendors

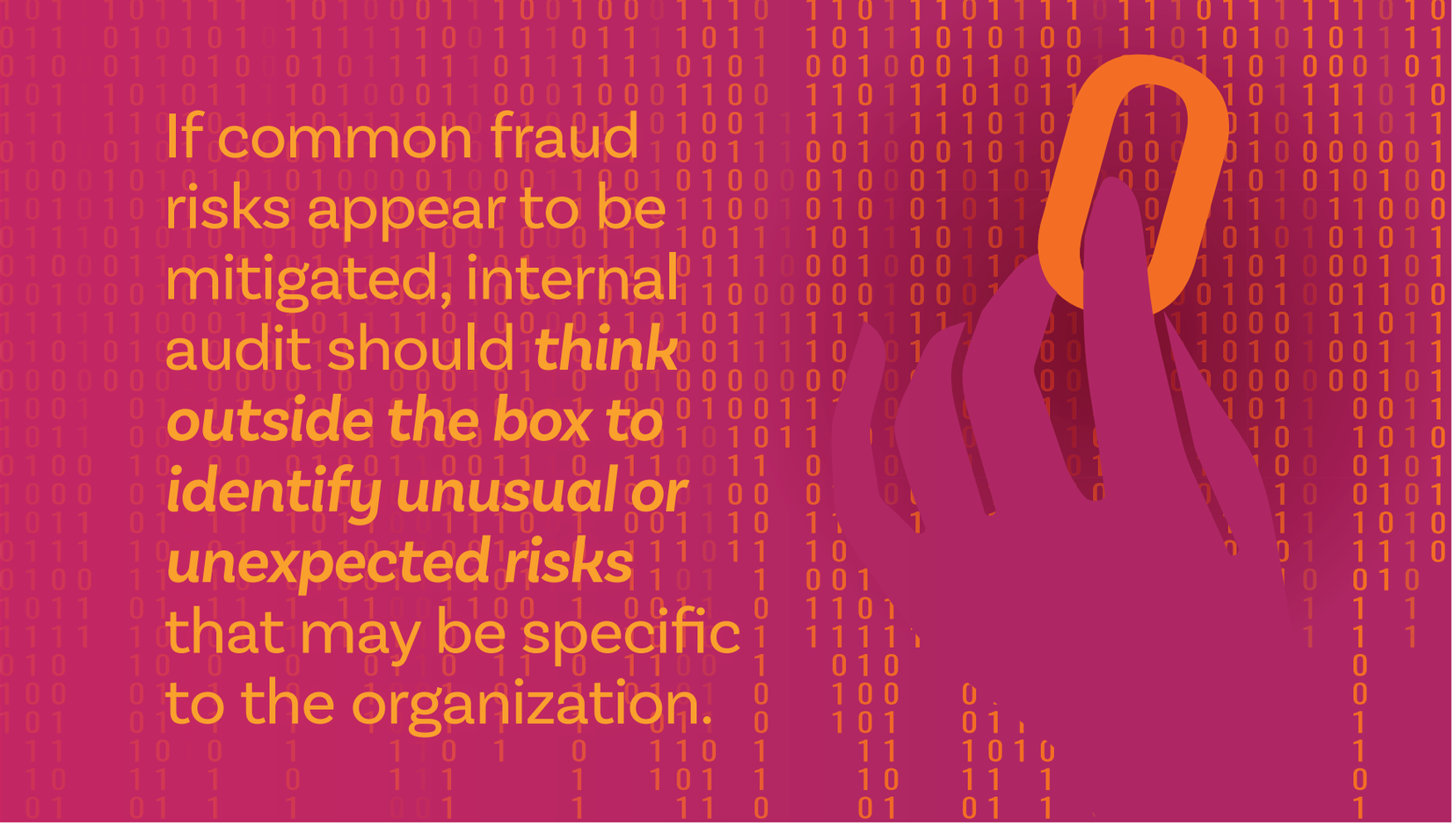
Fraudulent vendor activity can be a costly risk. This type of fraud occurs when an employee authorizes expenses and payments to fictitious vendors.

Internal auditors can use data analytics to check whether all vendors in the organization's database are legitimate. To identify potential fraudulent vendors, auditors should start by confirming that the vendor information is complete. Analytics tools can extract vendors with incomplete profiles, especially those with missing telephone numbers or tax ID numbers. Auditors should confirm that all the vendor addresses can be validated. Moreover, they should recommend stopping payment until the vendor information is completed and validated.

Auditors also should check for suppliers with limited address details, such as only having a post office address or having a residential address for a business location. Such suppliers can generate greater risk of fraud and financial loss to the organization. Using analytics to validate addresses can detect possible risks and identify opportunities to cleanse data to improve vendor master data.

Reviewing payments with little or no sequence between invoice numbers also can reveal potentially fraudulent vendors. Performing a routine trend analysis across key data sources may detect material control weaknesses. Benford's Law analysis may identify unusual distributions of random numbers such as invoice numbers and invoice amounts.

Additionally, auditors should confirm whether the organization appears to be the vendor's only customer or is one of a few customers. Finally, were the purchases legitimate, and was the purchasing organization getting the value it expected or was there something amiss? Weekend and holiday invoicing or vendor payments also may be a red flag worth investigating, particularly if certain vendor payments are habitually processed on nonbusiness days.



Internal audit should determine what it would take to perform a vendor spending analysis. This analysis should ask:

- Are invoices consistent month after month? Or are they typically quarterly or annual payments?
- Are vendor names very similar, such that payments may be erroneously duplicated?

A deeper analysis may be useful for payments to unknown vendors. Did these transactions start as a small payment that might stay under the radar and gradually increase? For example, an internal audit team using data analytics found that one of the company's software development vendors was based in a nearby residence. Looking deeper, auditors observed that spending on that vendor went from $2,000 per month for a few months to $10,000-$20,000 per month, and eventually increased to more than $100,000 monthly.

Payroll Schemes

Internal auditors can use data analytics to mitigate payroll schemes by identifying duplicate direct deposit account numbers, employee names, addresses, or phone numbers. For example, if auditors extract data about multiple payroll deposits to the same bank account during a single pay period, it may lead them to discover a potential fraud. Furthermore, this type of assessment may help the organization identify previously unknown related-party relationships such as nepotism.

Internal auditors also should confirm that appropriate segregation of duties are in place between the human resources and payroll functions. For example, responsibility for adding new employees should be segregated from the responsibility to pay employees to reduce the risk of ghost employees, falsified wages, or unauthorized adjustments.

Expanding Fraud Risk Assessments

Use of data analytics enables internal auditors to view 100% of the population, rather than a sample, and can greatly enhance the assurance the audit function can provide. If common fraud risks appear to be mitigated, internal audit should think outside the box to identify unusual or unexpected risks that may be specific to the organization, its employee base, and its industry. For example, access to customer records may not be appropriately limited to those with a "need to know." Without limits, any employee with access could leverage such information to engage in illegal activities such as insider trading.

As internal audit finalizes its audit plans for the year, it should identify opportunities to expand fraud risk assessments and develop analytics that can help reduce the risk of fraud. Auditors should brainstorm to determine additional activities that may be unique to the organization's environment and include them in the risk assessment and audit plan.

Alisanne Gilmore Allen, CIA, CRMA, CFE, CISA, is vice president, Risk and Compliance, at RGP in Santa Clara, Calif.

MIND THE GAPS *to the MAX*

NEW!

Internal Audit Foundation & Deloitte Research Report

Assessing Internal Audit Competency: Minding the Gaps to Maximize Insights

This groundbreaking report summarizes the global state of internal audit competency. It details where internal auditors across all levels, around the world, assessed their level of competency compared to The IIA's Internal Audit Competency Framework®. It's imperative for today's internal auditors to know their gaps in competencies and target areas for additional development.

Download your free copy today. ***www.theiia.org/CompetencyReport***

Internal Audit FOUNDATION

Deloitte.

Risk Acceptance

Internal auditors shouldn't be afraid to recommend this response.

Rick Wright

Internal auditors can inform stakeholders on the appropriate use of risk acceptance as an active response strategy and avoid the temptation for misuse. When navigating the risk landscape within an organization, management has a variety of risk responses in its risk management toolbox. Choosing the appropriate response depends on four things: the nature of individual risks, an organization's ability to exploit or absorb risk outcomes, associated opportunities and threats, and factors that influence risk outcomes. Such factors include impact, likelihood, speed of onset, and duration. Internal auditors can serve as thought partners with management when assessing the best risk response for a given issue.

A Variety of Risk Responses

There are four common risk response types: avoid, share or transfer, mitigate, and accept.

Avoid In some circumstances, the risk is so significant that management will decide to avoid the risk entirely. A good example of avoidance would be to completely disengage from a market due to geopolitical instability in a region of the world.

Share/Transfer Sometimes organizations choose to share or transfer risk with/to another party. This may be done by purchasing insurance policies or by forming business arrangements, such as joint ventures or other partnerships. A share or transfer risk response can be a good option when the other party has specific risk management competencies, such as familiarity in a particular geographical market (e.g., a U.S. based company that wishes to expand in a Latin American market).

Mitigate When risk management practices break down, new risks emerge, or risk profiles shift, mitigation often is an appropriate risk management strategy. Mitigation involves creating controls — or improving existing controls — to close a control design or execution gap. Mitigation tends to be the risk response internal auditors most frequently recommend as a course of action related to an audit observation. At times mitigation may be overused when other risk response types are better.

While it may seem like a passive management strategy on the surface, to optimize risk outcomes, *risk acceptance decisions may require active management.*

Accept Risk acceptance is used when other risk response options are unavailable or not optimal. Simply put, risk acceptance is a status quo risk response. Risk owners acknowledge the risk exists but "accept" the risk with minimal response. If the cost of other risk responses exceeds the value that would be gained, a risk acceptance strategy may be appropriate. While it may seem like a passive risk management strategy on the surface, to optimize risk outcomes — especially when risk is assessed as moderate or high — risk acceptance decisions may require active management.

A Real-life Risk Acceptance Story

A real-world example demonstrates how internal audit can actively guide management's effective use of risk acceptance to help organizations achieve the best risk management outcomes.

When I was working as an internal audit manager, I served alongside a couple of other managers, including our IT audit manager. I recall commiserating with the audit manager on occasion about troubles he had with his audit clients and getting them to provide timely action plans for audit recommendations. He complained that deliberations about audit observations and their associated recommendations sometimes dragged on for months after audit fieldwork was complete. Often, the delay was a result of hastily crafted action plans that did not address the risk at hand.

At some point, the IT department became aware of the "risk acceptance" approach to action plans and latched onto it with great enthusiasm. IT staff reasoned that if they just accepted the risk, the IT audit manager would have to defer to their judgment and risk response preference. Once word about the risk acceptance option got around within IT, this approach became almost the default standard and was used more frequently than the audit manager was comfortable with.

Fortunately, the manager is an auditor's auditor. Sensing an abuse of the system, he met with our CAE, and together they crafted a process to deal with risk acceptance

responses that resulted in much more rational outcomes.

The process they created hinged on management ensuring that when risk acceptance was the risk response of choice, key stakeholders were informed of and agreed with the decision. The risk acceptance process involved a formal document that was circulated among stakeholders outlining the issue, internal audit's risk assessment, management's decision for risk acceptance, and whether internal audit was in agreement with management's decision. In addition, if internal audit disagreed with management's risk acceptance response, auditors would articulate their reasoning.

For moderate assessed risks, the document would be circulated to the business unit leader for approval and signature. For high assessed risks, the document was circulated to the CEO for approval and signature. The risk acceptance document was attached with the final formal audit report and was shared with the audit committee.

This process changed IT management's position on the use of risk acceptance responses. As a result, the frequency of risk acceptance dropped considerably. Moreover, the process ensured that key stakeholders across the organization were aware of when risk acceptance was the chosen response and had the opportunity to dispute or concur with management's decision.

Actively Managing Risk Acceptance

Choosing the optimal response and follow up is critical to optimizing risk outcomes, which is the goal of risk management. While risk acceptance may at times appear to be a passive response, organizations should take a more active approach when risk acceptance relates to higher assessed risk. Likewise, risk acceptances should not simply end the discussion of risk response once the final audit report is issued. Instead, management should continue its risk management responsibilities by monitoring issues corresponding with risk acceptance responses when the risk assessment is high.

In its third-line position, internal audit can partner with management to ensure appropriate visibility of the issue over time in case there are changes affecting the risk. Depending on how the risk evolves and changes over time, management may need to adjust the risk acceptance response. Internal audit can help management determine when a different risk response may be warranted.

Get Comfortable with Acceptance

Some internal audit functions tend to shy away from advising audit clients and other stakeholders about the option of risk acceptance. Stereotypically, auditors tend to be risk-averse and more in favor of risk responses that reduce risk to the organization.

Yet, internal audit shouldn't be afraid to recommend risk acceptance when it's the right thing to do. A thoughtful and active approach to risk acceptance should be part of auditors' risk response guidance. Insisting on mitigation, when risk acceptance is the only practical response available, can damage the audit function's reputation and diminish its value proposition.

Rick Wright, CIA, is director of Internal Audit at Yellow Corp. in Overland Park, Kan.

A contradiction between weight and moisture data leads to fraud at a biomass plant. Anna Kon

Going Green

Northern Energy PLC, a company that provides electricity and heat in Lithuania, adopted an ambitious carbon emissions reduction program. The program includes an increase in the usage of biomass to produce energy.

Biomass is a mix of waste from forests and wooden waste. Combustion of biomass results in zero carbon emissions and contributes to achieving the program's goals.

Biomass is more expensive than fossil fuel, so it is critical to ensure that vendors provide quality biomass. Moisture is an important parameter for determining the quality of biomass — low moisture biomass produces more megawatt hours of electricity and heat.

Northern Energy had several costly experiences with dishonest vendors who would provide sales documents for high-quality biomass but, in fact, would supply a low-quality product that was wet, high-ash, and contained forbidden plastic or metal particles. After these incidents, the company took quality control into its own hands and implemented a biomass quality control process in both of its power plants.

Vendors deliver biomass by truck. The company established quality

control procedures that require fuel-handling facility personnel to obtain three samples of biomass from each truck that arrives. At the end of the shift, all samples that came from the same vendor are thoroughly mixed into a homogeneous substance. From this substance, personnel create two samples: One is sent to an accredited laboratory, and the other is stored for review. The laboratory conducts quality tests and determines moisture, ash level, and other parameters. The company uses the laboratory results to calculate the calorific value of supplied biomass and determine how much to pay the vendor.

Northern Energy's internal auditors were aware of the risks associated with biomass, so it was no surprise when they received a call from a manager at one of the power plants reporting an issue in need of an investigation. The manager reported that a fuel-handling specialist received data from the laboratory and noticed several delivery dates with abnormally low moisture percentages. The plant asked the laboratory to repeat the tests using the review samples, but the outcome was the same.

Claire Roos, one of the audit team members, was assigned to investigate the matter, alongside Peeter Janes, the new head of the fuel-processing facility. To conduct her investigation, Roos obtained all available dates from the laboratory, vendor invoices, and delivery documentation for the last four months. In addition, Roos was given access to surveillance cameras monitoring the biomass storage yard.

Roos reviewed the surveillance videos for the dates when anomalies were detected to determine if the established quality control procedures were being conducted correctly. She obtained entrance logs and weighing data, by truck and vendor, to determine their entry times so she knew the precise time she needed to review the surveillance videos to observe the unloading process.

Roos observed that no employees from the fuel-handling department came to take any samples of biomass from any load. She reviewed the entire shift and determined that delivery trucks kept arriving, unloading, and leaving without any samples being taken. Periodically, a bulldozer

Roos reviewed the entire shift and determined that delivery trucks ***kept arriving, unloading, and leaving without any samples being taken.***

Her analysis revealed a pattern where the weight of the biomass ***was not consistent with the moisture content of the delivery.***

would arrive, mix the biomass, and shovel some of it into feed conveyers.

For the dates in question, Roos confirmed that a power plant driver delivered bags with samples and vendor names written on them to the laboratory. She interviewed the driver, who stated that he always picked up the sample bags from the same location at the fuel-handling unit but had no idea how the bags got there.

Using data analytics, Roos compared different vendors — their trucks, dates, the weight of delivered biomass, and laboratory-reported moisture percentages. She observed that in one day, a single, fully loaded truck delivered an average of 22 tons per delivery. The moisture content of the biomass on this day was measured at 43%. However, the next day, the same truck delivered on average 36 tons of biomass per delivery despite having a laboratory confirmed moisture percentage of 15%. Roos knew that a truck that contains moist biomass must weigh more than the same truck that delivers dry biomass. Her analysis revealed a pattern where the weight of the biomass delivered was not consistent with the moisture content of the delivery.

Roos suggested that Janes assist with obtaining statements from employees. They agreed on what questions to ask in advance, focusing on whether employees were aware of the procedure requirements and why the required samples were not taken. A review of the statements revealed that the foreman at the power plant was assigning sample-taking responsibilities to employees daily. However, the foreman stated that no one was, in fact, taking the samples, which he blamed on increased workloads.

Roos and Janes visited the company's other power plant to determine whether it was executing the quality control procedures correctly or whether the employees were falsifying the samples. The investigation team was relieved to find that the plant executed the process as required and took samples, and that employees knew their duties. Roos decided to benchmark data from the well performing power plant with the one under investigation. The comparison revealed that in that same period, the same vendors were delivering biomass using the same vehicles to both plants. However, at the plant with appropriate quality control, the average moisture was approximately 52%, while at the plant under investigation the average moisture was only 26%.

Roos calculated the approximate loss for the four-month period under review to exceed a few hundred thousand euros. When Janes learned the extent of the loss, he asked Roos to support him in the second round of interviews with employees of the fuel-handling unit. During the interviews, some of the employees admitted that the foreman instructed them not to take samples from the arrived loads, but instead to take them from a pile of biomass in a corner indoors. The employees also stated that this arrangement did not apply to all vendors.

The foreman in question denied all accusations and claimed that he was not aware of his employees' actions. Despite suspicions, further investigations did not find direct connections between the foreman and the questionable vendors. The company dismissed the foreman and several employees. Also, the management of the power plant reviewed personnel needs, ensured that staffing per shift was sufficient, and conducted elaborate training on quality control requirements.

Anna Kon, CIA, CRMA, CFE, is a head of internal audit in Tallinn, Estonia.

LESSONS LEARNED

Business acumen and collaboration with management enable quick and efficient investigations. The auditor was familiar with biomass-related risks and processes and understood the business details. Management of the power plants were eager to solve the issue and stop losing money, so they actively engaged in the investigation. The auditor's expertise and the manager's commitment combined to produce an investigation that was conducted promptly and professionally.

Benchmarking data with a norm or another reliable and comparable data set can shed additional light on the data in question. Sometimes auditors study one specific population or set of transactions. However, juxtaposing a data set with another comparable set can expand outcomes and provide more insight. At Northern Energy, Roos knew there was a contradiction between weight and moisture data; however, looking into similar data from another power plant confirmed her suspicions and established the extent of the loss incurred.

Training and transparency are essential at all levels of the organization. It is not only important to instruct personnel, but also to explain the importance and meaning of controls. Fuel-handling personnel knew they had to take samples and send them to a laboratory, but they never comprehended the importance of the process. They did not imagine that by writing business names of vendors on sample bags consisting of biomass gathered from somewhere else, would be committing fraud. Also, they were not aware that by picking drier biomass they were causing the company to lose money and enabling a dishonest vendor to profit. Certainly, they hadn't thought of potential reputational harm to the company, which had an obligation to its vendors to conduct quality control.

Boldly

Preparing Better Professionals

CHANGE IS CHALLENGING. TRAINING IS TRANSFORMATIVE.

As the leading industry educator, The IIA delivers innovative, quality, and convenient professional development — covering an array of trending topics, training platforms, and skill levels. We want to ensure internal auditors worldwide can access the tools required to provide the highest level of assurance, insight, and objectivity possible.

Flex your mental muscles. *www.theiia.org/**Learning***

OnDemand | In-person | Online | Group | Conferences

The Institute of
Internal Auditors
Elevating Impact

A BRAVE NEW WORLD

With many offices beginning to reopen, organizations and internal auditors are returning to a very different business environment marked by new operational, workplace, technology, and social risks.

Neil Hodge Douglas Tocco

As the world approaches the second anniversary of the COVID-19 pandemic, organizations continue to grapple with several major risks that the crisis either created or exacerbated. Ongoing supply chain disruption is the risk that affects all organizations around the world to some extent, due to a potent mix of demand outstripping supply and COVID-19 flare-ups that may require further shutdowns. Rising energy prices also put manufacturing production and shipping in doubt.

Other key risks have grown in importance throughout the pandemic. Remote working has led many employees to become dissatisfied with their jobs and to question what it is about the work that makes them stay in their positions. Poor communication, lack of camaraderie, frozen (or even cut) salaries, coupled with limited opportunities for training or career development, have all helped fuel the Great Resignation.

Technology risks also have come to the fore, just as organizations are looking to invest to get ahead with the latest technologies. Home working has raised massive concerns over data security, prompting many organizations to devise controls to ensure employees do not put company or personal data at risk.

Employers face risks from societal trends that have gathered pace, too. While organizations have had policies to tackle incidents of racism, sexism, and inequality in the workplace, they are now also expected to take a vocal stand against such behavior in society.

On the following pages, *Internal Auditor* looks at the key issues arising from the pandemic that organizations are facing going into 2022 and the role that internal audit can play in addressing them.

Supply Chain Disruption

Practically every organization has been adversely affected by supply chain disruption in the past two years, and many have had to source new suppliers. Organizations have had to change quickly, with management and executives being forced to focus on the immediate risks to ensure the survival of the business.

However, two years on, some organizations may still be involving senior management in day-to-day operational issues, putting the long-term strategy of the business in jeopardy. Gary Connors, partner at Gloucester, U.K.-based business consultancy Oliver Wight, says the supply chain crisis has created a "panic stations" situation. Connors cites this as an example of a "compressed" organization — a strategy that can be counterproductive. "We need businesses to be 'decompressed' so that executives are freed up to deal with strategy and think further ahead, developing assumptions and scenario plans," he says.

Leading companies are already adjusting their supply chains to

turn disruption into a competitive advantage. Clothing company Levi Strauss & Co. has realized benefits by diversifying its supply base. The company has decided not to source more than 20% of its products from any one country to avoid concentrations and to be less exposed to bottlenecks and production capacity. Proctor & Gamble, meanwhile, has used its global footprint — and global muscle — to make its supply chains more flexible so that it can shift sourcing when necessary to avoid bottlenecks.

For the auto industry, a "just-in-time" operating model — the practice of ordering products only when needed — is no longer practical for systems that are capital intensive, require long lead times, and are interdependent on other industries. Ford Motor Co. has said the pandemic "has fundamentally changed the way we're thinking about procurement and design."

Others have had to take more drastic action. Germany's Opel, a unit of Stellantis, the company that owns Jeep and Fiat, said in September that it would shut down one of its factories until early 2022 because of a shortage of semiconductors, furloughing the plant's 1,300 workers.

However, experts say that while organizations are right to review risks within their supply chains, they may be overlooking the vulnerability of the infrastructure that supports them. "Even if the supply chain is technically working, it amounts to very little if the infrastructure that supports it isn't working," says Rich Cooper, global head of financial services at software vendor Fusion Risk Management in Rolling Meadows, Ill. "In many countries, manufacturing has been able to continue, but restrictions on movement and travel have meant that goods and supplies just can't be accessed because they are stuck at ports, freight terminals, warehouses, and airport cargo holds."

Dan Zitting, chief product and strategy officer of New York-based governance, risk, and compliance software vendor Diligent, says to navigate supply chain disruption successfully, internal audit should quantify the risk at a much earlier point. Auditors can do this by looking at the disruption of labor in regions where the organization knows it is dependent on its supply chain. For example, a notable spike in coronavirus cases that forces the public to remain at home may create supply chain issues.

"Even if the supply chain is technically working, it amounts to very little ***if the infrastructure that supports it isn't working.***"

RICH COOPER
Global Head of Financial Services
Fusion Risk Management

Zitting says to take a proactive approach to risk mitigation, internal audit can assess risk upfront and put preventive measures in place early. "When disruption hits, it is important to have a third-party risk management program in place, running appropriate risk assessments to evaluate potential issues in those suppliers," he explains. "Organizations also should assess how much risk they can take on and if they are willing to put automatic triggers in place if needed." For example, the organization could set a trigger at which it will raise prices or when contracts with back-up suppliers and vendors will be brought forward.

The New Work Environment

Prolonged absence from the office has changed the relationship employees have with their colleagues and managers, as well as their employers. At its best, remote working has empowered people to act independently, make their own decisions, and work more flexibly; at its worst, however, it has hindered collaboration, decreased trust, and increased employees' likelihood to leave.

Johnny C. Taylor Jr., president and CEO of the Society for Human Resources Management based in

Alexandria, Va., says the changing dynamic between employers and employees has sowed three problems. First, retaining key people and talent is now more difficult. "There is a lack of 'stickiness,' which means it is easier for people to move to other employers," Taylor says. Without a shared dynamic or emotional attachment to one's place of work, changing jobs can "simply come down to who pays more and who can offer the best work/life balance," he explains.

Second, remote working means there is a risk of organizations becoming less innovative. Virtual meeting tools such as Teams and Zoom do not emulate the type of work environment where employees know what is going on, why strategies are enacted, and the challenges teams are facing, Taylor explains. "Remote working means people are missing cues, nuances, or important background information that you only get when people are in the same room, so ideas are not being generated or challenged," he says.

Third, remote working may contribute to a lack of diversity. "Working from home stifles relationship building and visibility," Taylor says. "If a project needs doing, organizations tend to use people who already have experience or a pedigree, which means other candidates are overlooked and opportunities for staff with untested talents dry up."

> "If you bring employees back, make sure they are ***working in teams doing group work to rebuild a collaborative dynamic.***"

JOHNNY C. TAYLOR JR.
President and CEO
Society for Human Resources Management

Remote work also may lead to lack of inclusion and inequity, such as inequitable treatment or access.

Taylor says organizations should designate days when all staff should come back to the office, and it should be done as soon as possible. "If you bring employees back, make sure they are working in teams doing group work to rebuild a collaborative dynamic," he stresses.

While human resources (HR) departments will inevitably take charge of return-to-office policies, internal audit can inform the process by flagging potential problem areas that have been brought to its attention. Auditors can ask if HR has plans to monitor or evaluate how successful or problematic these policies have been in practice.

Working from home has created other risks that are likely to be front of mind in 2022 — notably data security — but the measures organizations are taking to protect themselves are creating additional problems. Manoj Satnaliwala, an internal audit consultant based in Dallas, says employers have tried to push accountability for managing IT security and data privacy onto employees. Some have required employees to sign contracts that make them responsible for data leaks linked to their devices and activities. "This is little more than making workers accountable for the failings of the organization," Satnaliwala says.

Instead, he says internal audit should recommend that the IT department works directly with employees to address security settings. "Employees aren't IT security experts," Satnaliwala says. "Most workers will be happy to take precautions and follow protocols, but they need to be aware of what these are and how to follow them."

Technology Risks

The pandemic has taken organizations' focus — and budgets — away from investing in new technologies and leveraging their capabilities. However, boards also need to beef up their understanding of IT and data risks, while internal audit should continue to push for better data governance.

"Presently, too many organizations simply allow third parties access to data without questioning why they need it, what they might

be doing with it, and whether it is deleted after they use it," Satnaliwala says. "Internal auditors need to push their boards to be more aware of what data they have, where it is kept, and who has access to it." CAEs also should examine what IT services are outsourced and the vendors' access to data.

Michael Phillips, an adjunct professor at DePaul University's College of Computing and Digital Media in Chicago, says organizations need to get better visibility into how well their data is protected and who is in charge of protecting it. One of the biggest concerns is organizations' increased reliance on cloud computing.

"The cloud is a common risk for many organizations because they misunderstand what a cloud service provider is responsible for," Phillips explains. "A cloud vendor is responsible for the security of the cloud, while the company using the service is responsible for the security of the data it puts in the cloud." He notes that depending on the cloud relationship — software-as-a-service, infrastructure-as-a-service, or other arrangement — organizations may be heading for trouble if they don't have IT people who understand cloud architecture and security.

> "Internal auditors need to push their boards to be more aware of ***what data they have, where it is kept, and who has access to it.***"

> "A few years ago, it was the case that if you were compromised, it took ***weeks, or even months, for an exploit to manifest itself. Now it is seconds.***"

MANOJ SATNALIWALA
Internal Audit Consultant

MICHAEL PHILLIPS
Adjunct Professor
DePaul University
College of Computing and Digital Media

Ransomware also poses a significant threat, Phillips says. The U.S. Federal Bureau of Investigation warns that there are now 100 different strains of ransomware circulating around the world. The surge in attacks has been fueled by the "triple extortion" ransomware technique, which targets the organization whose data was stolen, as well as its customers, vendors, or business partners.

"A few years ago, it was the case that if you were compromised, it took weeks, or even months, for an exploit to manifest itself," Phillips explains. "Now it is seconds." The high risk and frequency of occurrence has led some insurers to stop paying ransom payments in some regions, tighten policy requirements, and increase the cost of ransomware policies.

Phillips says there is plenty of scope for internal audit to promote better awareness and security to combat these risks. Internal audit should begin by ensuring that IT security is part of its remit when carrying out reviews — and not just for financial systems. "They need to look at operational risks much more closely, as the financial systems typically sit on the same untrusted

computing environments as other systems," he says.

Societal Change

Recently people have been more open about showing their political colors, as well as speaking out about the issues in society that they care about — or hate. Campaigns around gender rights, Black Lives Matter, and #MeToo are issues that people care about and expect employers to care about, too. Other issues, however, such as anger against mandatory COVID-19 vaccinations and the rise of extremist political views, have proven more divisive. Such discussions are part of a greater focus on corporate environmental, social, and governance practices, something that investors and regulators also are expecting companies to address.

Silvia Gonzalez-Zamora, head of the Inclusion and Diversity Service at KPMG in Canada, says in recent years there has been "a heightened social consciousness" of the inequalities and inequities that traditional structures and systems have created. Equity-deserving groups, such as Black, Indigenous, people of color, women, 2SLGBTQI+, and people with disabilities and neurodiversity, have had unequal access to education, jobs, housing, and health care. These issues are too great to ignore. "Organizations are slowly learning that the risk of a lack of social justice, losing biodiversity, or protecting sexual predators could bring their employer brand, product reputation, and business stakeholders' trust to the brink of collapse," she explains.

According to Gonzalez-Zamora, organizations can act to tackle equity across talent management, sustainability across product development, and respect across inclusive cultures before the challenges are insurmountable. She says these issues are quantifiable risks that organizations can measure, monitor, and change by focusing on tangible actions, and that internal audit has a key role to play.

"Internal audit is tasked with objectively reviewing and assessing the operations and business tactics, and it is the function that can evolve processes, practices, and policies to a new level and toward a better future for all," Gonzalez-Zamora says. Internal audit can lead the way for organizations "by setting the standards of greatness, justice, quality, and efficiency with a social and environmental conscience."

To learn new skills and acquire experience and understanding, audit teams need to design and develop an internal audit life cycle with a diversity, equity, and inclusion (DEI) lens, she says. Internal audit should apply a DEI lens to the full audit life cycle for both DEI- and non-DEI specific engagements — for example, when conducting risk assessments, scoping/planning, staffing an engagement, interviewing, and selecting samples.

Additionally, internal audit needs to conduct specific engagements focused exclusively on DEI, such as around culture and conduct, human resources, performance management, stakeholder engagement, and workplace misconduct investigations, Gonzalez-Zamora advises. CAEs also could help develop a customized training plan bridging the internal audit methodology with DEI principles.

"The biggest risk that organizations face today is doing nothing, not speaking up, and staying the same," Gonzalez-Zamora says. "Those that purposefully and meaningfully support organizations, charities, and campaigns to help create equitable and sustainable environments, cultures, products, and services will be the ones that will stand tall against the test of scrutiny and time."

"The biggest risk that organizations face today is ***doing nothing, not speaking up, and staying the same.***"

SILVIA GONZALEZ-ZAMORA
National Inclusion and Diversity Practice Leader
KPMG Canada

Rising to the Challenge

As in the previous two years, internal audit functions will need to step up to meet the challenges that their organizations will face as a result of the lingering fallout from the pandemic. While hopes rise that the world — and corporate life — will return to a greater degree of pre-COVID-19 normality, it is obvious that several key risks that surfaced during the initial lockdowns will require internal audit's continued input if they are to be successfully mitigated and controlled.

Indeed, forward-thinking CAEs may be able to take advantage of opportunities arising from these risks: Better data governance may free up funds to invest in better IT solutions, while embracing social justice and greater diversity and inclusion may help attract new talent and help retain key staff, for example. Meanwhile, re-examining supply chains may lead to cost reductions and improvements in operations. There is certainly scope for internal audit to review the strategic possibilities that each of the key risks creates.

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

While hopes rise that the world — and corporate life — will return to a greater degree of pre-COVID-19 normality, ***it is obvious that several key risks that surfaced during the initial lockdowns will require internal audit's input*** if they are to be successfully mitigated and controlled.

attr@cting the next generation

To pass the torch to the next generation, practitioners need to connect with students in high school and college, create worthwhile internships, and rethink their retention strategies.

Diane Sears

ew people grow up saying, "I want to be an internal auditor." People tend to gravitate toward the profession midway through their careers, often discovering it by accident or being volunteered to take on internal audit responsibilities as part of a management training track. This poses a challenge for the future as internal audit teams look to fill positions when Baby Boomers and Generation Xers retire and Millennials become in charge. How will Generation Z (Gen Z) learn about the profession?

Part of the issue is that internal auditing seems to be a well-kept secret, says Mara Ash, CEO of BFS Strategic Partners in Austin, Texas. The other part is that the profession is not marketed in a way that makes it sound "sexy" enough to pursue.

"Internal auditing is fun," Ash says. "It's interesting. There are different challenges every day, and in public sector auditing, you're contributing to society — you're making the world a better place. What's not to like? The problem is, we don't present it that way."

Ash, who spoke about the next generation of internal auditors at The IIA's 2021 International Conference, says auditors tend to use technical terms to explain what they do. That approach is not working, she insists. "We talk about doing 'intensive analysis' and those types of things — and frankly, that's why people think we're accountants."

Alternatively, people associate auditing with uncovering fraud, Ash says. "Everybody loves that; everybody wants to find an 'I gotcha' case. But 98% of what we do is not fraud and not an 'I gotcha,' it's evaluating programs and processes and public agencies that make people's lives better. That's what makes it sexy, and that's where we lose sight of how to engage young people," Ash points out.

Focusing on the "why" behind internal auditing will help attract people from Gen Z, who are driven by purpose and are more globally connected and competitive than previous generations. They want to know they are making a difference in whatever career they choose — and able to do so right away.

Focusing on the "why" behind internal auditing will help attract people from ***Gen Z, who are driven by purpose and are more globally connected and competitive than previous generations.*** They want to know they are making a difference in whatever career they choose — and able to do so right away.

Start Early

It will take time to lower the average age of the internal audit profession, which today stands at 43.9 in the U.S., according to job search website Zippia, which uses machine learning techniques to collect data on millions of careers. Ash explains why that age is significant: "When you start thinking about that, depending on which country you're in, you really only have 10, maybe 15 years to cultivate the new generation of auditors. If we don't, we're going to see huge gaps."

To attract members of Gen Z, who were born roughly between 1997 and 2012, it's important to reach them early, even as early as high school. CAEs can encourage their teams to conduct outreach in their own communities.

"I tell CAEs that they need to get into their schools and do career workdays," Ash says. "You can ask, for example, 'How many of you have an issue with the department of motor vehicles and think it takes forever to get your license? Yeah, we do too. So guess what? We went in and audited that, and we reduced your wait time by an hour. How about that? Am I impacting your life? Am I making it better? All right, who wants to join me?' It really is about those kinds of conversations."

The timing is now crucial because on top of an aging workforce, many

countries around the world are also dealing with high employee turnover and labor shortages. After experiencing a wake-up call during the COVID-19 pandemic, many people are looking for work that brings meaning to their lives instead of just providing a paycheck. They want to have an impact, Ash says.

"They're thinking, 'I need to feel good about my job. I also need to get paid adequately and be treated like a human being,'" she explains. "That's what younger generations want. They want that flexibility; they want the ability to have an impact. And, truly, that's something internal audit does well."

Rethink Marketing

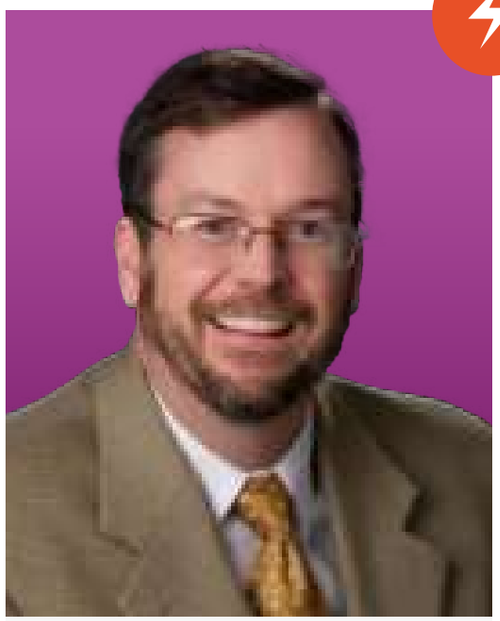
In a perfect world, the profession would have its own streaming TV drama — a way to educate people about what internal auditors do day-to-day and how they make the world a better place. Ash points to the increased interest in jobs like criminal investigation after the launch of the "CSI: Crime Scene Investigation" TV franchise, or the uptick in people wanting to be morticians after watching "Six Feet Under."

With or without a sudden interest from Hollywood, internal audit needs a marketing makeover, says Steve Goodson, an internal audit consultant and a lecturer at the University of Texas (UT) at Austin. "People know what lawyers do, and what accountants do, and what doctors do," he says. "But for some reason, even internal auditors have trouble explaining what they do. We really need an effort to help outsiders understand what we do."

In fact, Goodson has spent the last six years spreading the gospel of internal auditing, one student at a time, at UT Austin. He teaches internal auditing at the McCombs School of Business, where his course is part of a five-year integrated bachelor's and master's degree program in accounting. The program is designed to produce candidates for the Big Four accounting and audit firms: Deloitte, EY, KPMG, and PwC. His classes fill up with about 140 students a year, with roughly one-third of those who are pursuing a master's degree in the program. "In many cases, they have never heard of internal auditing," he says.

Goodson persuaded the registrar's office to allow his class to be part of the fourth-year accounting curriculum when students are still making career decisions, instead of the fifth.

> "People know what lawyers do, and what accountants do, and what doctors do. But for some reason, ***even internal auditors have trouble explaining what they do.***"



@Steve Goodson
Internal audit consultant; lecturer at the University of Texas at Austin

That strategy seems to be working, he says. About 5% of his students go to work as internal auditors in private industry or seek positions in risk advisory with the Big Four firms.

Goodson also offers students hands-on experience as part of the curriculum: Students are required to spend a semester working in the community on an actual internal audit project. Groups of two to four students plan and execute an audit engagement and have taken on everything from line-of-duty death benefits for corrections officers to income and expenses related to National Collegiate Athletic Association programs.

When he's not teaching or working with the local IIA chapter, Goodson looks for opportunities to speak to young people about the profession. "I actually came up with a slogan and have a logo that says, 'Internal audit makes a difference,'" he says. "I give out stickers with the logo on it — and hats, and water bottles, and coffee mugs." This year he was asked to participate in an orientation panel for new students in the business school. "Anybody I shook hands with, I gave them a sticker and said, 'Don't forget about internal audit,'" he says.

Offer College Internships or Co-ops

For about five years, two members of IIA–Toronto have been in a strategic relationship with the nearby University of Waterloo, working to help students recognize internal auditing as a career option. Like Goodson in Austin, they have seen a heavy emphasis on preparing students to go to Big Four firms for entry-level jobs or internships — or what Canada and the U.K. call co-op programs.

"The sheer size of these firms creates a consistent demand for jobs," says Tony Malfara, a retired KPMG Canada partner and chair of IIA–Canada's Advocacy and Academic Relations Committee. "With the University of Waterloo, we've been working jointly with the business community and predominantly the big financial institutions to convince them to take the students in."

Malfara's colleague on the Waterloo project, Colin Shaw, has put this into practice at OMERS, an organization that delivers defined benefit pensions to Ontario municipal employees. Shaw serves as senior vice president and head of global audit.

"Everybody's got to start somewhere," Shaw explains. "We take co-ops on a regular basis." Shaw knows from experience — he was a co-op student, himself, in England. He says the students are able to get involved in testing and meet senior executives across the organization, offering them valuable exposure to the profession. "They either figure out, 'Hey, this audit thing is not for me' or they get bitten by the bug and run with it," he says.

Such partnerships between the business and academic communities are crucial to forging future generations of internal auditors, Malfara says. The goal of the IIA–Toronto partnership with Waterloo is to encourage the academic institution to devote a full program to the profession, once a high enough volume of students are interested in internal auditing. "I'd say we're maybe 30% to 40% along that journey," Malfara says.

Malfara describes today's situation as simple supply and demand: "The demand comes from the businesses, the supply comes from the university, and the students are the inventory," he explains. "We need the students to understand that internal auditing is an option for a rewarding and well-paying career and a means to get to the top of an organization."

> "We need the students to understand that internal auditing is an option for ***a rewarding and well-paying career and a means to get to the top of an organization."***

@Tony Malfara
Chair, Advocacy and Academic Relations Committee, IIA–Canada; retired partner, KPMG Canada

Both Malfara and Shaw are committed to working with both sides of the equation to cultivate the supply and demand at Waterloo and beyond. "The hope is that once we've sort of bottled the secret sauce, we can then translate that to other universities across Canada as well," Shaw says.

Strategize Ways to Retain Gen Z

Once organizations do manage to attract Gen Z workers to internal auditing, they face another challenge: retaining them. Holding the long-term interest of the youngest generation is not the same as it was when the Baby Boomers and their parents started careers with the aim of staying in one job for long enough to receive a gold watch and a retirement party.

As a speaker on intergenerational human capital workforce engagement, Mariam Riza in Melbourne, Australia, has been studying what makes this generation tick. She calls them "Gen Zed" in the British pronunciation as she explains the differences between the generations

How The IIA is working to build the profession

The IIA promotes the adoption of an internal audit curriculum worldwide to help educate the next generation of internal auditors. With two IIA-endorsed academic programs, The IIA textbook, its "course in a box," and a variety of other resources, The Institute is helping teachers prepare students for a career in internal auditing. Further, through the Internal Auditing Education Partnership Program, The IIA has endorsed 56 universities across 15 countries teaching multiple courses or offering certificate or degree programs in internal auditing.

The Institute also is working closely with its chapters and affiliates to reach even more students at both the high school and collegiate level. IIA volunteers and staff promote awareness of internal auditing through a variety of initiatives, such as outreach to educators to support them in teaching or presenting information on the profession in their classes, clubs, or campus organizations. IIA chapters and affiliates also contribute by sponsoring student IIA memberships, sharing internship opportunities, and establishing mentor programs at the local level.

On a more macro scale, The IIA hosts the annual Internal Audit Student Exchange for students around the globe. During the pandemic, The IIA shifted to hosting the complimentary event virtually and added a second event in April. The September 2021 virtual event reached nearly 500 students from 90 universities across 30 countries.

and why the global financial crisis that started in 2008 had such a profound effect on Gen Z.

"Gen Zeds coming in, they've seen their parents go through the global financial crisis and Asian financial crisis, so they're driven," explains Riza, who is CEO of management and training consultancy Wattleshire. "They are hyper-competitive because Gen Zeds were born with technology, so automatically their sphere of influence or the sphere they're influenced by is significantly larger."

That makes internal auditing a good option for Gen Z workers because the job offers them quick access to top leaders, from whom they can learn and be mentored. However, their view of the corporate world may be different from that of their predecessors, Riza says.

Gen Z is willing to climb the corporate ladder, but their timeline may be faster than that of the organization they work for, she explains. "They're looking at different avenues to succeed to get a portfolio or exposure to a variety of industries for depth and breadth. What we see as perhaps attrition is really them sampling as many things as possible so they get that repertoire of skills."

Riza says she started receiving calls from a professional accounting association in Australia about seven years ago. Accounting firms were troubled by an attrition problem, with younger workers leaving about every two years. "I realized it wasn't necessarily an attrition problem, but just that business models weren't keeping up with the times," she says. For Gen Z workers, careers look more like lattice work than ladder structures.

"In the last few years, a significant change we've seen is that accounting software and auditing software have changed the way we do business, so they're coming in because they want to learn the industry. But they're not staying," Riza says. "Instead of waiting 25 years to make partner, they're learning the ropes through these established companies and then using technology to set up their own firms about seven years later, once they have some experience."

This trend is clashing with the "silver tsunami" of people retiring, Riza points out. That makes it more urgent that organizations learn how to harness the ambitions of Gen Z while still honoring the intentions of these leaders of tomorrow.

"It's really simple," she says. "Provide a transparent pathway to learning and development opportunities." Instead of showing young workers the self-paced learning management system and wishing them well, today's leaders need to be more hands-on.

"It's about sitting down with them with a plan and saying, 'I want you to be part of the organization,'" she explains. "If you want to keep them for seven years, build a plan for that seven years and run through it with them, saying, 'This is where you are now. This is what you're going to achieve in six months, two years, seven years.' Sit with them on a regular basis to see how they're tracking against it."

It's also important to help young auditors collect a variety of skills, Riza says. "Don't train them to do only, say, forensic audit or IT audit, but show them the pathway so they stay longer to attain all kinds of different training."

Riza advises organizations to put in place several other strategies to keep Gen Z interested:

- Make the organization's stand on social issues apparent to them, and allow them to pursue volunteer ventures as part of their work.
- Market to Gen Z where they actually are, such as social media sites like TikTok.
- Allow Gen Z to be entrepreneurial and solve problems inside the boundaries of the organization, which could mean having them find ways to automate clunky audit processes.
- Adopt technology to augment internal audit processes and communication, showing that the organization is willing to adapt to changing times.

"It's not the fact that Gen Zed is changing companies," Riza says. "It's the fact that the business models themselves are changing because of globalization of the supply chain and other factors. Every generation comes in lobbying for change. This generation is just the current one. What's actually changing is the business models of the future."

Shine a Spotlight on Internal Auditing

The first step to attracting tomorrow's talent is to pull the work of internal auditing out of the shadows and into the spotlight. Ash, who often speaks about "future-ready" internal auditors, says one of the greatest benefits of the position is the way it exposes professionals to every aspect of an organization.

"There's not one CEO of any Fortune 500 company who hasn't done a rotation in internal audit," she says. "And why? Audit is the one position, other than the CEO, that touches every single department in an organization. So I tell folks all the time, 'You shouldn't be recruiting accountants. Accounting and finance are not the only operations in an organization. You need to be recruiting from across the spectrum because all of those skills are going to be helpful.'"

Ash and others say the best internal auditors are excited about solving puzzles and finding answers to problems — traits that are needed in numerous careers. Talk about that to young people, and watch their faces to see if it ignites interest.

"We have to change how we talk about the process to say that we, as internal auditors, get to take challenging data and come up with creative solutions," Ash says. "We get to tackle problem-solving every day. Highlight the process, but in a positive way, rather than the drudgery of the past."

"We have to change how we talk about the process to say that we, as internal auditors, get to ***take challenging data and come up with creative solutions.***"

@Mara Ash
CEO, BFS Strategic Partners
Austin, Texas

Diane Sears is founder and president of DiVerse Media LLC in Orlando, Fla.

ADVANCING CLIMATE ACTION

INTERNAL AUDITORS ARE UNIQUELY POSITIONED TO FURTHER THEIR ORGANIZATIONS' CLIMATE CHANGE JOURNEY.

Israel Sadu
Douglas Tocco

The many recent extreme weather events experienced all around the globe have yet again raised debate on climate action. And following the COP26 Climate Change Conference in Glasgow late last year, the Paris Agreement — the international treaty on climate change — is gaining momentum. All eyes are on the policy and investment decisions that will chart a course to net-zero carbon emissions by 2050. According to the Energy Transitions Commission, a global coalition of energy producers, industrial companies, and financial institutions, reaching this goal will require an investment of about $1 trillion to $2 trillion annually.

Complex climate policies and their business impacts may overwhelm organizations in determining their deliverables and future strategies. Leveraging its unique position in providing advisory and assurance services, internal audit can help companies and investors in a holistic way to prepare them for their climate action journey. This, in turn, will help internal audit provide assurance around control processes with complete, accurate, and reliable information.

A Scenario-based Climate Risk Assessment

From a business perspective, climate change risks broadly involve transition risks such as climate laws and policies that affect how companies transition to a low-carbon economy, and physical risks that include damage to fixed assets or supply chain disruptions. There are also possible opportunities, such as reduced operating costs through greater efficiency and expanded markets for existing or new products.

It may not be easy for companies to visualize the wide range of impacts of emerging climate change risks. Scenario analysis is a valuable tool for understanding risks and consequences. Internal audit can help companies validate the scenario analysis models used for evaluating climate-related risks and opportunities for their compliance with the organization's internal control framework. The core strength of internal auditors to collect, understand, and analyze voluminous data will be an advantage in calibrating the scenarios and assessing impacts.

Because the application of scenario analysis to climate-related risks and opportunities is very recent, internal auditors may need to gain additional insights through a multipronged approach. This includes participating in the industry-led debates on scenario-based climate risk assessment, working with business entities' climate scenario analysis teams, and securing a seat at the discussions on governance of climate scenario analysis.

Climate Considerations in Business Strategy

Climate change is a potential strategic risk to companies and should be managed accordingly. For example, the board should build into the business strategy climate considerations such as pivoting the business model away from carbon-centric sectors, climate-resilient risk management, altering the range of products or services and supply chains or changing manufacturing locations, and determining capital allocation patterns.

To provide assurance in this area, internal audit must have a thorough understanding of the nature of climate change risks impacting the business, and above all, an innovative mindset and the ability to sensitize management and boards. This is possible through providing a spatial view of potential risks and their outcomes and championing a system of integrating the results of climate risk scenario analysis within business strategies and decisions.

A Financial Impact Assessment

New technologies aimed at mitigating climate change risks through adaptation and mitigation activities could impact business operations, the company's capital, and eventually the financial statement, including, for example:

- Revenue due to transition and physical risks, which may affect demand for products and services and their pricing.
- Capital expenditure plans and the level of debt or equity needed to fund these plans.
- Assets impairment, including goodwill, changes in useful life, fair valuation, impairment calculations, provisions, and contingent liabilities arising from fines and penalties.
- Debt and equity structure, either because of increasing debt levels to compensate for reduced operating cash flows, or for new capital expenditures or research and development. There also could be changes to capital and reserves from operating losses, asset write-downs, or the need to raise new equity to meet investment.

Investors expect material climate risks to be reflected appropriately in audited financial statements. Depending on the geographical location in which the entity operates, it is essential that organizations undertake the financial impact assessments of projects dealing with climate-related risks in alignment with the evolving climate-centric regulatory environment. Internal audit can assist in this area by evaluating control design effectiveness and working with the external auditors.

Promoting Disclosures

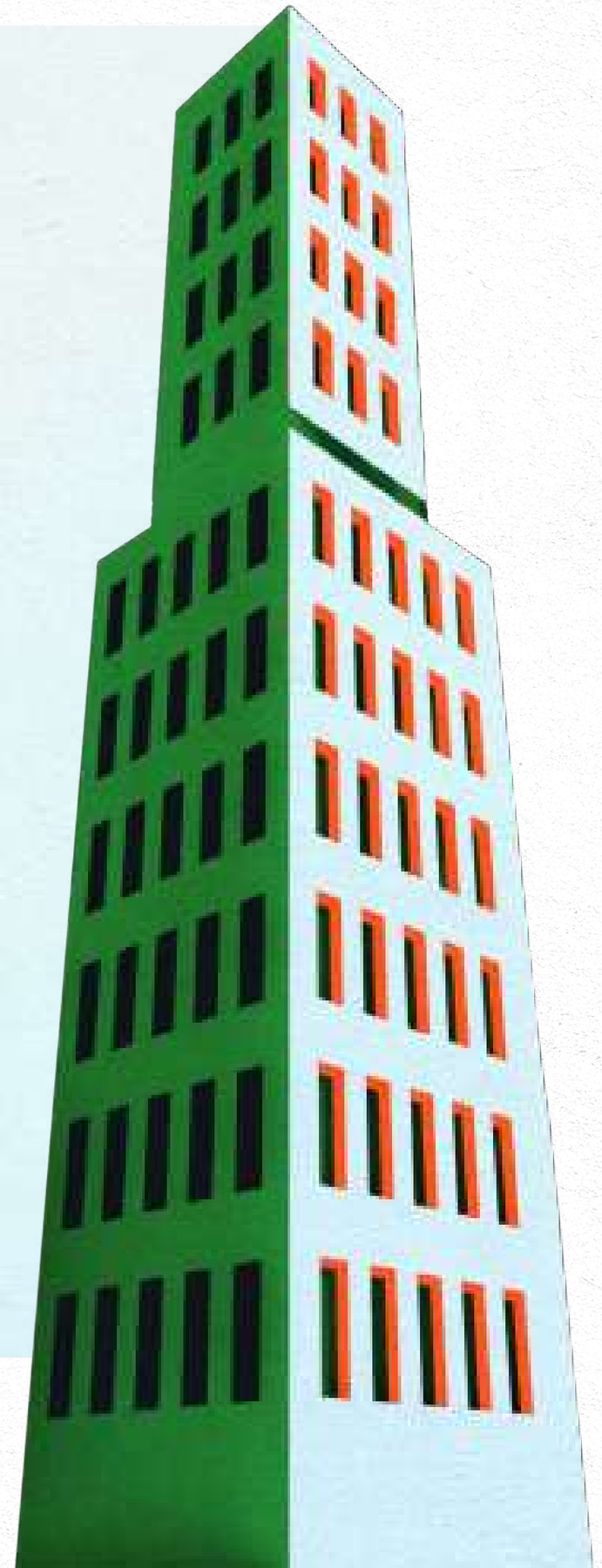
Under disclosure or nondisclosure are often a product of poor climate change governance and, consequently, cause difficulties in engaging capital markets to smooth the transition to a low-carbon economy. According to ClientEarth, an environmental law charity based in the U.K., 90% of financial accounts and audit reports for the 250 largest publicly listed companies in the U.K made no reference to climate risks or their financial impact in their climate-change related reporting (2019-2020). There is a growing demand for increased voluntary and mandatory environmental and sustainability disclosures from a range of participants in the financial markets.

Companies that make some attempt at climate change disclosures

Climate Competency

There are several resources that internal auditors can reference on their journey to become more climate competent:

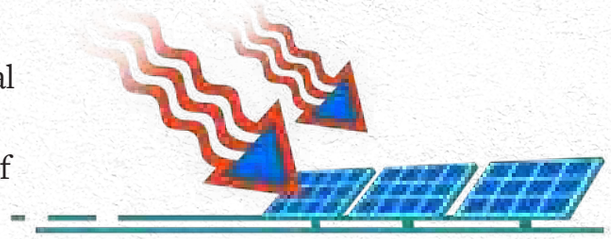
- International Sustainability Standards Board (ISSB)
- The U.S. Securities and Exchange Commission's Climate and ESG Task Force
- INTOSAI Working Group on Environmental Auditing
- The Financial Conduct Authority
- Prudential Regulation Authority
- EU Corporate Sustainability Reporting Directive
- COSO, Applying Enterprise Risk Management to Environmental, Social and Governance-related Risks, October 2018
- World Economic Forum, How to Set Up Effective Climate Governance on Corporate Boards: Guiding Principles and Questions



are facing increasing litigation over the accuracy and reliability of the disclosures. Conversely, robust disclosures build increased confidence regarding the accuracy and reliability of the information revealed. Today, despite wide acceptance of the Task Force on Climate-related Financial Disclosures recommendations, the format in which companies report remains largely voluntary, and there are varying degrees of compliance. Internal audit can help companies promote disclosure by:

- Validating the reporting process, from source to report, to assess the cost and efficiency of reporting.
- Identifying gaps in the company's disclosure of its current efforts and future commitments, processes or controls, and metrics used for reporting to boards.
- Validating whether the reporting standards used are complete and accurate — not only to ensure accuracy in external reporting but to confirm that the envisioned cost benefits are met.
- Verifying if internal audit, the compliance team, and relevant third parties, such as the external assurance provider, have been engaged to review the quality of the reporting processes.

INTERNAL AUDIT CAN HELP BOARDS ASK THE RIGHT QUESTIONS, UNDERSTAND THEIR DUTIES WITH REGARD TO CLIMATE CHANGE DISCLOSURE, AND INCORPORATE CLIMATE RISKS AND OPPORTUNITIES THAT ARE INTERTWINED WITH THE WORK OF THE ORGANIZATION.



On the nonfinancial reporting front, in the absence of reliable baselines and metrics for reporting, internal auditors should help organizations develop and benchmark them by documenting methods followed for identifying, collecting, measuring, and reporting on sector- and risk-specific metrics.

Strengthening Oversight

Integrating oversight and management of climate change into the governance structure helps ensure that climate change risks are strategically managed. In 2021, KPMG questioned more than 160 U.K. business leaders, representing a range of industries, on a set of environmental, social, and governance questions. When asked if climate change was a top priority, 82% said it was already being actively discussed, or on the boardroom agenda. However, when asked if they had a clear view of the risks ahead and how to tackle them, only 8% of businesses reported having a full-fledged plan in place, with 89% in early-stage discussions, and 3% not at all.

Internal audit can help boards ask the right questions, understand their duties with regard to climate change disclosure, and incorporate climate risks and opportunities that are intertwined with the work of the organization. They should also prepare the audit committees for external reviews and audits, as the latter increasingly integrates climate change risks.

Next Steps

COVID-19 highlighted the perils of failing to prepare — resulting in about a 3.4% drop in the world's gross domestic product (GDP) in 2020 — and its impact is far from over, according to an estimate from Statistia, a business data platform. The Swiss Re Institute's stress-test analysis reported in April 2021 that the world economy is set to lose up to 18% of the world's GDP from climate change by 2050 if no mitigating actions are taken.

Internal audit is uniquely positioned to advance climate action by being "insightful, proactive, and future-focused," as stated in The IIA's Core Principles for the Professional Practice of Internal Auditing. Key to achieving this is for chief audit executives to empower audit teams to become climate competent through equipping them with enough competencies and skills to assess the impacts of climate change risks on the business environment and develop confidence as trusted advisors.

Internal auditors should seek out potential opportunities to work on assurance and advisory engagements related to climate change. Such engagements may be triggered by changes in business or simply management's desire for internal audit's perspectives. To begin, internal audit departments should develop and maintain a risk-based audit universe of clients' business operations with significant environmental sustainability risks for annual audit planning. Depending on an organization's climate risk maturity, the engagements could be a climate change risk-focus thematic review across the audit universe, or as a component of every engagement. A combination of the two may be a better approach as maturity increases.

Internal audit cannot afford to stand alone in this endeavor. Sustained partnerships and collaborations with chief risk officers, management, boards, and external auditors will be a catalytic force to accelerate the organization's climate action journey — and it needs to begin now.

Israel Sadu, PHD, CIA, CRMA, CISA, is an auditor with an international organization in Geneva.

AGILE

Auditing Using Scrum Techniques

Increasing agility in the audit process using a supportive framework can help auditors deliver more value and remain relevant in a rapidly changing environment. **Clarissa Lucas**

Change has always been constant, but in recent years the pace of change has increased exponentially. Because of this, organizations are seeking ways to respond by improving efficiencies and making decisions faster, all while reducing expenses. Meanwhile, business partners are speeding up the processes by which products and outcomes are delivered. Given this current state, how can internal auditors keep up?

Internal auditors are finding they can leverage concepts like Agile and scrum in response to rapid change and to better serve their customers. Scrum is a framework used to guide teams to work together to achieve a common goal, usually through iterative delivery of value. Internal auditors can apply an Agile mindset and supporting scrum framework to help prioritize value for stakeholders.

An Agile Mindset

Agile auditing enables auditors to:

- Focus on areas of greatest value and highest priority.
- Respond more easily to change.
- Gain greater client buy-in and collaboration.
- Communicate results timely to stakeholders.
- Drive accountability for delivery.
- Reduce wasted time.

To effectively apply a scrum framework to internal auditing, auditors need to understand the values on which an Agile mindset is based. According to *Scrum: The Art of Doing Twice the Work in Half the Time*, by Jeff and JJ Sutherland, it's about "people over processes; products that actually work over documenting what that product is supposed to do; collaborating with customers over negotiating with them; and responding to change over following a plan."

For example, the concept of valuing working products over extensive documentation doesn't mean auditors need to abandon documentation altogether. It means auditors shouldn't lose focus on the end goal for the sake of documentation.

In an audit, the product is assurance or actionable insights. Applying this to the Agile value results in assurance or actionable insights over extensive documentation. Internal audit can increase its agility and value by continually anchoring back to the profession's overarching goal of providing assurance to stakeholders. When audit teams find themselves spending more time perfecting documentation for internal recordkeeping than providing assurance to stakeholders, they can remind themselves of this Agile value and redirect their focus.

When audit teams find themselves ***spending more time perfecting documentation for internal recordkeeping than providing assurance to stakeholders,*** they can remind themselves of this Agile value and redirect their focus.

Mapping Scrum to Internal Auditing

In the spirit of continuous improvement, Agile teams can take another step on the journey by applying a scrum framework. There are several foundational elements of scrum that can be applied to an audit.

The team. Effective Agile teams have three main attributes:

1. A collective commitment to achieving the team's goals.
2. Members who have the skills necessary to perform the work.
3. Self-organization.

Two key roles within the team are the scrum master and the product owner. The scrum master coaches the team on scrum techniques, while the product owner is accountable for the product (e.g., audit deliverable). In most audit organizations, the product owner is the audit leader or executive, and the scrum master is typically the audit senior or audit project manager. Other team members primarily include audit staff; however,

depending on the engagement, clients may be included on the team, as well.

Sprints. Traditional scrum activities include sprints, which are timeboxes during which a team works collectively to deliver a working piece of software. Teams use sprints as regular checkpoints with clients on the product they are delivering. This enables teams to pivot and respond to changes and results in a continued focus on delivering value to the client.

An Agile audit team defines a sprint as a timebox during which a team works collectively to deliver actionable insights, linking back to the Agile values. The key concept is that at the end of the sprint, the audit team delivers something of value to the client. That delivery is the "definition of done" for the sprint.

An Agile audit team frequently delivers actionable insights to key stakeholders throughout the course of the audit. Instead of delivering the totality of results at the end of a three- to six-month audit, the team delivers insights along the way at scheduled points in time. This way, information provided to clients is timely and less likely to be stale by the time clients receive it.

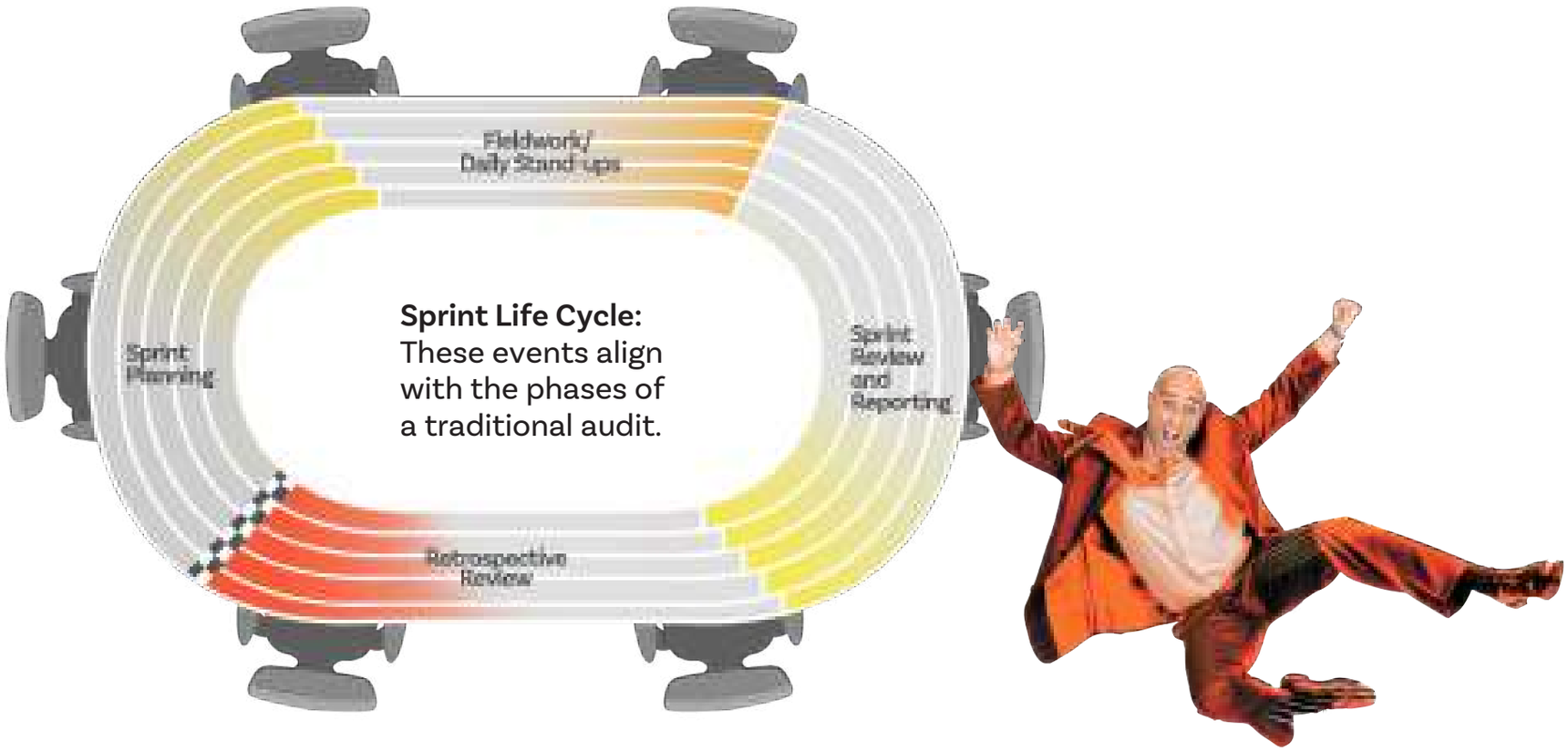
Timeboxing: Agile team divides work into epics and prioritizes high-risk or high-value epics.

To timebox an audit, the Agile team starts by breaking down the work into smaller, manageable chunks, called epics. Before the sprint begins, the team develops the product backlog, which can be done in an hour or two for a one-month sprint. The product backlog is a list of work to be completed for delivery of a product. In the context of an audit, the product backlog (sometimes referred to as the audit backlog) is the list of work to be completed to execute the engagement and deliver results.

To develop the backlog, the audit team collaborates with clients and other auditors who have perspective on the auditable entity to identify key focus areas. The team may decide to assign one key risk to each epic, or find some other way of dividing the audit's scope into manageable areas of focus. The team prioritizes the list of epics, moving the items of greatest risk or highest value to the top of the list.

Sprints last one month or less, and all sprints in the audit are of equal length. Before each sprint begins, the team determines which epics can be accomplished, focusing on the highest-priority items.

The sprint is complete when the timebox expires. At that time, the team moves any



Sprint Life Cycle: These events align with the phases of a traditional audit.

incomplete tasks back to the product backlog and prioritizes them for the next sprint.

The Sprint Life Cycle

To ensure delivery of value to the clients on time, Agile teams can leverage the sprint life cycle, which includes sprint planning, daily stand-ups, sprint review, and a retrospective review. These events align with the traditional phases of an audit: planning, fieldwork, and reporting.

Sprint planning and fieldwork. Teams identify the scope of work for each sprint in a planning session. The entire team, both auditors and clients, participates in the session. Objectives of the session could include:

- Identification of key risks and controls relevant to the process under review.
- Determination of testing procedures and requests/evidence needed to complete testing.
- Alignment on the sprint goal and "definition of done" for the sprint.

Identifying these objectives in the sprint planning session creates clarity on the focus areas, the expected deliverable, and what it takes to get there. Having the client actively participate in the session not only creates buy-in, but also leads to a better understanding of expectations and reduced confusion over the course of the sprint.

The audit staff actively participates in each sprint planning session, ***providing insight and gaining an understanding of the scope and sprint goals.***

Traditionally, a project manager would develop the plan for the audit and involve the audit staff once the plan was finalized and fieldwork began. Using an Agile approach, the audit staff actively participates in each sprint planning session, providing insight and gaining an understanding of the scope and sprint goals. This creates stronger buy-in and clearer expectations among the audit team, as well.

After defining the sprint goal, the team breaks down the work into manageable tasks and adds them to the sprint backlog. Each task includes a "definition of done," so it's clear when the task is complete.

Scrum teams use tools to manage the sprint backlog and create visibility to the team. Some teams use physical whiteboards with tasks written on notecards, while other teams use tools that replicate this concept digitally. With the increase of geographically dispersed teams, digital tools are instrumental in the process. Using a

control test as a task, the team creates a card for the control test and includes the "definition of done." It's also helpful to include the steps needed to get there. In this instance, the workpaper must be documented, submitted for review, and approved by the appropriate individual.

From here, in a traditional audit, the project manager assigns controls to each staff member, and they go their separate ways, testing controls in a silo. This can result in duplicative efforts, which wastes valuable time. Each team member documents findings identified and submits them to the project manager for review. Once the project manager reviews the finding, he or she sends it to the audit leader for final review. This could take days or weeks to complete.

When leveraging a scrum framework to audit with agility, the audit team continues to collaborate throughout fieldwork. Each team member can see what their teammates are doing, what they're learning, and the roadblocks encountered. They identify and address duplicative efforts and discuss findings collectively. Each team member is empowered to provide his or her insights. Relevant stakeholders participate as well, resulting in delivery of real-time feedback from all key parties. Findings are ready for clients in a matter of hours or days, instead of weeks.

Daily stand-ups. Scrum teams use daily stand-up meetings to create an environment for, collaboration. Stand-ups are held to identify impediments to meeting the sprint goal and create clarity on the most important item for each team member to focus on that day. To accomplish this, the team answers:

- What have you accomplished since the meeting yesterday?
- What will you accomplish by tomorrow?
- What impediments are in your way?

By creating visibility of impediments to the entire team, rather

than only to the project manager, auditors can get feedback from others who may identify solutions. Daily stand-ups enable a team to identify problems early and reduce wasted time. They also facilitate the team's ability to self-organize by allowing each member to decide which card to focus on next. Cards in the backlog are not assigned to team members by the project manager. Instead, team members self-assign a task once each has availability to perform it.

Sprint review and reporting. At the end of a traditional audit, the team and client have a closing conference to share the audit report before finalizing it. This closely aligns with the sprint review when leveraging the scrum framework, where the two parties inspect the sprint output with key stakeholders and determine what to do in the next sprint. The primary difference between a traditional closing conference and the sprint review is the additional goal of determining what to do in the subsequent sprint. To do this, the team (audit and clients working together) reviews the list of prioritized audit scope areas/epics, adjusts the priority as needed, and decides which epics can be accomplished in the upcoming sprint.

Retrospective review. The final stage in the sprint life cycle is the retrospective review. Agile audit teams perform blameless retrospective reviews at the conclusion of each sprint to identify ways to increase quality and effectiveness. Participants in retrospectives can consist of the audit team, client team, and other key stakeholders. The team identifies a few improvement opportunities from the retrospective review and implements those moving forward.

A Proactive Response

Implementing an Agile mindset and applying a supporting framework to the audit process can create many benefits, including reduced expenses, increased efficiencies, faster decision-making, and proactive response to change. Internal auditors must focus on value provided to key stakeholders to remain relevant in this rapidly changing environment. Increasing agility in the audit process can help teams deliver that value, and leveraging a scrum framework is a tool that can support the auditor's Agile journey.

Clarissa Lucas, CIA, CISA, is the technology audit director at Nationwide Insurance in Columbus, Ohio.

Getting Personal

Focusing on relationship building as a strategy can make a big difference in how internal audit is perceived and improve engagements overall.

Jami Shine and Seth Peterson

Audit leaders often overlook the relationship side of auditing as they focus on technology advances, emerging risks, and industry trends. However, the "people element" of auditing will always be essential, positioning internal audit for failure or success. Auditors can use multiple best practices to develop stronger, more collaborative relationships with their audit clients and produce more effective audits. Aligning with the values and culture of the organization, engaging in the company's culture, staying connected in between audits, and building trust are key to effective auditor-client relationships. These principles also help to address common challenges in auditing such as overcoming negative perceptions of audit and promoting client engagement in the audit process.

Aligning With Organizational Values and Culture

Aligning the audit department with the organization's core values and culture is necessary for building strong working relationships. Auditors can take three simple steps to get a thorough understanding of the values and culture.

Do the Research. Most organizations post plenty of information about their values and culture on the company website. Audit team members also can glean vital information about culture through conversations with department heads or more experienced auditors, while new auditors can review the results of any culture audits that have been performed. Another option is for auditors to work with human resources, which often is tasked with driving core values and culture, to increase their understanding.

Be an Active Observer. Auditors can find clues about cultural norms through observation. For example, at QuikTrip, a privately held corporation based in Tulsa, Okla. that specializes in gas station convenience stores, employees are highly social in the hallways. Some employees arrive at work 30 minutes early to "make the rounds" and engage in small talk on their way to their desks. In this type of culture, it could be perceived as rude or uncaring for an auditor to walk down a hallway without talking to anyone. The conversations aren't as much about gaining information as engaging in the corporate culture and demonstrating that employees care about each other.

For auditors, being an active participant in the organizational culture is a key component of being visible and helps business units see auditors as people.

Be a Participant. Participating in events and activities outside the audit department helps immerse auditors in the corporate culture and offers greater insight into shared values. At QuikTrip, the entire internal audit team attends the company's Manager Development Conference, a week-long culture boot camp. For auditors, being an active participant in the organizational culture is a key component of being visible and helps business units see auditors as people.

Once auditors understand the core values and culture, they should focus on building relationships based on those shared values. Auditors tend to socialize primarily among themselves, especially at large organizations. However, they should engage with people throughout the organization to build healthy relationships before, during, and after the audit.

Many organizations have a core value of service to the community. At The First National Bank in Sioux Falls, S.D., employees are committed to their community, and the internal audit team helps lead that charge by being active participants in service projects. They participate in Habitat

for Humanity build projects, rake leaves for the elderly, serve food at shelters, and volunteer in the classroom for Junior Achievement or mentoring programs. Similarly, at QuikTrip, auditors are encouraged to serve on nonprofit boards and fundraising committees and as leads in community service projects. Team members may even have nonaudit skills they can share with the organization or community. For example, QuikTrip's CAE is well-known for putting his construction skills to use during United Way events.

Engaging in the Company's Culture

Auditors strive to add value and improve operations enterprisewide. To be effective, auditors must demonstrate they are on the same team as the entire organization. Sometimes reinforcement is needed to help other areas of the organization understand this team approach. Auditors can use a variety of techniques to show their support for the organizational team.

Attend Social Events (even when it's uncomfortable). Auditors should make an effort to attend birthday parties, baby showers, and happy hours. These are great

Auditors strive to add value and improve operations enterprisewide. To be effective, auditors must be able to demonstrate they are on the same team as the entire organization.
Sometimes reinforcement is needed to help other areas of the organization understand this team approach.

opportunities to network outside of the department. QuikTrip's auditors are known for cards and gifts tinged with their unique sense of humor, which helps establish them as relatable to their clients.

Serve on Company Committees. Diversity, equity, and inclusion initiatives, charity fundraising activities, and social committees are a great way for internal auditors to network and build relationships. Auditors at First National Bank often are involved in these types of internal activities. Serving on committees allows auditors to pursue their nonaudit interests, which can provide job enrichment, increase job satisfaction, and motivate auditors in their daily responsibilities.

Seek Group Volunteer Activities. Volunteer leadership positions in local organizations enables auditors to network with their community and learn from others who aren't in the audit field. Volunteer positions also can provide auditors with opportunities to make decisions and manage processes that fall outside of the norm for their roles. Volunteering together is even more rewarding. For example, QuikTrip's internal auditors shop together each year for Toys for Tots, which is a great bonding activity that reinforces a team mindset.

Present at Employee Orientations or Other Events. Many auditors struggle with their clients not knowing what they do, which can lead to challenges or even resistance during the audit process. Giving presentations during new employee orientations or International Internal Audit Awareness Month is a great way to educate clients on audit's collaborative role and also to sell the audit group as helpers.

First National Bank has gotten creative with its Awareness Month activities. Events have included auditor trivia, critical-thinking exercises, and root cause analysis examples — with food and drinks generally a key draw to the events. The department has even been able to play on and debunk some stereotypes of auditors to create a fun atmosphere for the events. These activities not only help build relationships throughout the organization but also improve the perception of the internal audit function.

Audit by "Walking Around." Auditors often learn more about issues that require assurance or advice — emerging risks, potential fraud, or operational deficiencies — from their internal networks rather than through any key performance indicator or risk questionnaire. Knowing what's going on in the organization is critical to building an appropriate audit plan. In a virtual environment, auditors can still reach out to their nonaudit colleagues via chat or email. A quick check-in to see how someone is doing can go a long way toward maintaining a relationship.

Serving on committees allows auditors to pursue their nonaudit interests, which can ***provide job enrichment, increase job satisfaction, and motivate auditors in their daily responsibilities.***

Staying Connected and Building Trust

Forming strong relationships establishes trust. This trust, in turn, creates the opportunity for business unit leaders to be open and honest. This openness manifests itself through the discussion of upcoming projects or process changes. Ultimately, auditors seen as a trusted resource will have greater risk awareness, and individuals will seek them out to help them through challenges. There are several ways auditors can effectively stay connected and build trust.

Leverage Technology. The COVID-19 pandemic has created new challenges with staying connected in the organization. While many auditors have been successful in maintaining relationships, they should continue to nurture and enhance those relationships. Whether an audit team has remained remote, transitioned to a hybrid arrangement, or

fully returned to the office, technology continues to be an important consideration in how teams connect with each other. The most successful audit groups are the ones that have leveraged technology to continue this personable audit approach.

Throughout the pandemic, teams were forced to get creative when in-person socializing was turned on its head. As individuals had a need and desire to feel a connection, some teams turned to virtual check-in meetings or virtual happy hours. Colleagues began asking people how they were doing, beyond the normal pleasantries. As organizations move forward, audit leaders shouldn't lose sight of the impact of these meetings.

Provide Recognition. Technology offers a nearly free way to express gratitude to co-workers and show appreciation. Sending emails to wish someone a happy birthday, celebrate a work anniversary, or celebrate a promotion can lift someone's spirits. Taking the time to recognize co-workers helps break down barriers, change people's perception of auditors, and allow auditors to further connect.

Auditors have to deliver difficult information at times, but there is nothing that prevents them from delivering positive news, as well. There is no impairment to independence or objectivity in recognizing solid work by others in the organization, but unfortunately, auditors often shy away from the positive. Highlighting the positive even helps show that auditors are looking at the full picture and can provide some confidence to those carrying out daily activities.

Both QuikTrip and First National Bank encourage auditors to provide this recognition, as merited. For instance, First National Bank has a "Virtual High Five" program that auditors use to recognize outstanding colleagues and clients. Auditors also can offer recognition to colleagues verbally or through LinkedIn or via emails to the employee and the employee's supervisor. These types of activities require minimal effort but help overcome the perception that internal audit is only interested in policing compliance.

Maintain Contact. One way that auditors can build relationships throughout the organization

is by staying in contact with clients between audits. It can be challenging to find time and opportunity to connect, especially in a large organization. However, an exchange doesn't need to be time-consuming to be meaningful. Something as simple as an occasional chat message or email — or stopping by someone's office to say hello — can help maintain healthy working relationships between audit cycles. If auditors are only friendly during an audit, it can create the perception that they are insincere, so taking a genuine interest in clients both during and after an engagement is essential to creating trust. Knowing names also can go a long way; a simple hallway greeting demonstrates that auditors remember and value former audit clients.

Promote Client Engagement in the Audit Process. A final way to build trust and increase effectiveness through relationships is by engaging the client in the audit process. Audit procedures that are second nature to internal auditors may seem overwhelming to clients. Clients may feel auditors are trying to "trap" them or that they are creating meaningless busywork for them. Even worse, they may feel auditors aren't in touch with the most critical objectives and risks, resulting in observations that are blown out of proportion or that don't create value for the business. Auditors should engage the client in every stage of the audit process.

Recognizing How Collaboration Improves Internal Audit

Within the role of internal audit, the importance of relationship building cannot be overstated. Often overlooked, it's the personal side of auditing that allows auditors to make a difference in organizations. The ultimate benefit of establishing trust and strong relationships is more effective audits. Through these relationships, auditors are able to build stronger cooperation with the business units. Management can demonstrate greater openness over control issues, and there may be better alignment with other assurance and risk functions to minimize duplication of efforts.

Trust also enables internal audit to work collaboratively with the first- and second-line functions within the organization. If those functions see internal audit as a threat and hide control gaps and issues, it will lose its effectiveness. In a healthy culture, all three lines work together to promote effective risk management and operations. Internal audit can build healthy relationships with other risk functions through open discussion, frequent contact points, collaboration, and not caring who gets the credit. For example, if a second-line function identifies a significant control gap, internal audit can build trust by giving the function credit for the finding in the audit report and even pointing out steps they are already taking to remedy the issue.

Within organizations, internal auditors are uniquely positioned to evoke positive change but will be ineffective in doing so if they do not first focus on how they make their clients feel. The relationship component may be the single most effective way to exponentially increase internal audit's impact. It is only when clients trust internal audit's desire and ability to help them achieve their goals that auditors can truly become trusted advisors.

It's the personal side of auditing that allows auditors to make a difference in organizations. ***The ultimate benefit of establishing trust and strong relationships is more effective audits.***

Jami Shine, CIA, CRMA, CISA, CRISC, is a corporate and IT audit manager for QuikTrip Corp., based in Tulsa, Okla.

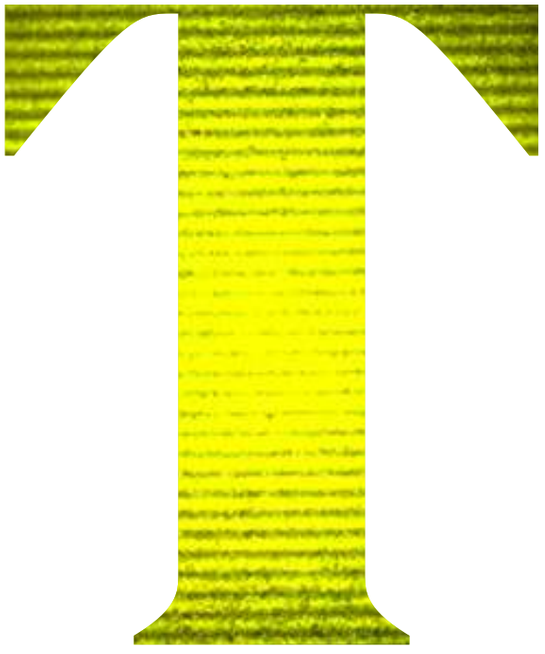
Seth Peterson, CIA, QIAL, CRMA, CISA, is the senior vice president and chief risk assurance executive at The First National Bank in Sioux Falls, S.D.

Auditing AI Governance

As organizations rely more on artificial intelligence, internal auditors should focus on governance principles to assess oversight of these applications.

Kitty Kay Chan and Tina Kim

Douglas Tocco



echnology advances in recent years have triggered a surge in artificial intelligence (AI) across many different applications to improve the quality of people's lives. For example, AI-powered medical diagnostic systems provide early disease detection to save lives, fraud protection systems identify unusual electronic payment transactions to combat identity theft, and ridership applications increase the efficiency of transportation services.

What these AI applications have in common is a processing capability that simulates human intelligence to analyze their environment and make decisions. These capabilities have led to a greater need for oversight of AI. AI governance provides frameworks and processes for directing AI applications in accordance with organizational goals, user expectations, laws, and ethical behavior. As with other areas of governance, internal auditors can help their organization determine whether AI governance is designed and implemented appropriately.

The Importance of Governance

As with human decision-making, AI systems sometimes produce decisions that fail to meet their intended goals, which can expose organizations to risk and harm users and communities. The potential for error and its impact is what makes auditing AI governance important. For example, in 2018, Reuters reported that Amazon had to discontinue its machine learning-based recruiting engine after its AI was found to be biased against women. In the same year, researchers at the Massachusetts Institute of Technology and Stanford University found that three commercially released facial-analysis programs demonstrated both skin-type and gender biases.

Regulations for overseeing AI applications are limited by what has been referred to as a "pacing problem." As AI technologies advance quickly, it may not be feasible for these regulations — which require a long and thoughtful vetting process — to catch up and provide oversight. Auditing AI governance can help bridge this gap.

Potential voluntary labeling also makes auditing AI governance important. The European Commission's 2020 white paper, On Artificial Intelligence — A European Approach to Excellence and Trust, suggests the use of voluntary labeling for low-risk AI applications. Such a labeling system would provide a means for organizations to inform users that their AI-enabled products and services are trustworthy as a result of following sound AI governance. Because the information on the label would be self-disclosed, it would not be subject to regular examination by regulatory agencies. AI governance audits could increase users' confidence in that information.

In addition, some public-sector agencies use voluntarily reported information on a range of governance topics together with information such as required regulatory filings to check for noncompliance with regulations. For example, the U.S. Securities and Exchange Commission examines voluntarily reported corporate environmental, social, and governance information to check its accuracy and take appropriate enforcement action. An AI governance audit could help companies ensure the information disclosed is accurate and consistent.

Principles Are the Foundation

Although most countries do not have AI laws and regulations, various entities have developed principles to support the responsible use of AI. These principles provide the foundation for a good governance framework. Examples include frameworks developed by:

- **Governmental bodies**, such as the Organisation for Economic Co-operation and Development's Principles on AI and Singapore's Model Artificial Intelligence Governance Framework.

- **Companies**, such as Google's AI Principles and the Microsoft AI Principles.
- **Industry associations**, such as the International Technology Law Association's Responsible AI Policy Framework, and COSO's Framework and Principles to Help Implement and Scale Artificial Intelligence.

There is no common set of AI principles because different sectors have specific operational needs and evolving technologies. Thus, governance will depend on each organization's objectives.

However, some essential building blocks of AI principles are common across different governance frameworks. A shared characteristic of these principles is their support for social well-being and sustainable development. Internal auditors can classify these principles into four categories:

- Accountability.
- Fair and inclusive.
- Transparent, explainable, and robust.
- Privacy, security, and safety.

Auditors should ensure that, as part of good governance, the organization has clearly stated objectives to help achieve its mission and that its AI principles are aligned with those objectives. Moreover, the organization should have policies to ensure the use of AI is consistent with those principles. Auditors should apply the AI principles in auditing governance practices.

Different functions within an organization may leverage their own AI systems, and those managed by third-party vendors, to support operations that are unique to their specific needs. Internal auditors should inquire if third-party vendors conduct audits on their AI governance practices.

AI governance audits should start by identifying all of the AI applications that the organization has deployed and uses. This inventory should include information such as purpose, deployment date, department ownership, internal and external users, third-party vendors, and a unique identification number for each system.

AI applications with the highest predictive power may leverage techniques that make systems less transparent and explainable. In other words, ***a system that is the best at predicting outcomes may not meet other AI principles.***

Accountability

Effective governance requires accountability. This is a special challenge with AI, given that multiple parties are usually involved and it often is not clear what the metrics of success are.

A key measurement of success for AI systems is their predictive power. Application developers and managers are typically evaluated based on how accurately the system can make a prediction. However, AI applications with the highest predictive power may leverage black box algorithms and techniques, which make systems less transparent and explainable. In other words, a system that is the best at predicting outcomes may not meet other AI principles.

To evaluate whether there is an effective governance framework to support accountability, auditors should check whether processes are in place to clearly explain who is accountable for various parts of the AI system. They should determine what each individual is accountable for as well as goals to measure against.

For example, internal auditors should examine whether outcomes are consistent with AI principles, such as building a fair and robust AI algorithm. They should determine whether employees' responsibilities are clearly delineated and documented, staff are qualified and trained to perform their work, and key performance indicators are measurable and hold individuals accountable.

Fair and Inclusive

The fairness and inclusivity principles are linked to fundamental human rights. AI systems should empower everyone, regardless of gender, race, religion, disability, and sexual orientation. Auditors should look for evidence that the governance framework ensures the organization's use of AI does not breach these rights.

Putting such processes in place requires developers to test and correct for potential biases introduced by the data set used to train the system to make decisions and predictions. Auditors can check whether developers are training the system with data that captures characteristics of the entire population rather than just a subset of the population. They should determine if developer teams reflect appropriate diversity to ensure that different opinions and perspectives are considered. For example, training an AI system using data obtained mainly from one racial or income group could lead to biased outcomes for others in the population.

Transparent, Explainable, and Robust

In terms of transparency, auditors should ensure that the governance framework supports stakeholders' access to accurate, timely, and relevant information. Being explainable requires being able to explain to stakeholders about decisions the AI system makes in both technical and nontechnical terms, depending on the stakeholders' needs.

Having timely access to accurate and relevant information does not necessarily ensure something is explainable. This is because technical explanations are not useful in helping nontechnical stakeholders understand why and how the AI system produces decisions. Furthermore, stakeholders' appetite for technical explanations varies across organizations.

A stable AI system is one for which the decision does not change significantly when the information being entered is modified slightly.

To evaluate whether there is an effective governance framework to support the explainable, auditors should check whether:

- A process is in place to translate technical information into nontechnical terms.
- Sound communication channels exist for stakeholders to provide feedback, along with a process for such feedback to be considered and incorporated.

Stakeholders' feedback makes it possible for auditors to evaluate whether there is an appropriate level of transparency and understanding.

In terms of robustness, auditors should look for a governance framework that supports stable and reproducible decisions made by AI systems. A stable AI system is one for which the decision does not change significantly when the information being entered is modified slightly. Reproducibility means that the same AI system

can be built by external parties, using documentation and data provided by the developer, and still generate the same decisions as the original system.

Auditors should check if there are guidelines in place requiring the organization to test the stability and reproducibility of an AI system, including reporting of unusable and irreplaceable results. For example, auditors could look for whether the organization makes available files that replicate each step of the AI system development process.

Privacy, Security, and Safety

Large volumes of data can be used to retrace and de-anonymize data of individuals, raising privacy concerns. Appropriate levels of data privacy governance protect the rights of users to make their own decisions about who can process their data and for what purpose. Good governance on security measures for the infrastructure of AI systems safeguards data from unauthorized access.

To evaluate whether there is an AI governance framework in place to support data privacy and infrastructure security of the AI system, an auditor could first determine whether there are authentication standards, data encryption processes, and tools to protect data erasure. The auditor also should check that there are monitoring tools and standards to track system access and keep records of adjustments made to data and algorithms. Next, the auditor can evaluate whether these standards and processes meet industry norms and customers' needs.

In terms of safety, auditors should look for a governance framework that can access, monitor, and mitigate the potential risk of AI-driven outcomes that could raise safety concerns. One example is determining whether there are processes, such as adversarial testing and patrolling for data poisoning, to continuously monitor the safety of the system. Adversarial testing probes weaknesses in, and evaluates the robustness of, an algorithmic decision-making model by purposefully running examples aimed at deceiving the model into providing incorrect results. This method couples these examples with a monitoring algorithm to track the model's performance. Patrolling for data poisoning aims to catch any external attacker or malicious insider who seeks to undermine the performance of an AI model by tampering with the data used to train the algorithm. Auditors also can check whether there are processes, such as human intervention, to tackle unforeseeable risks triggered by inaccurate predictions by the AI system.

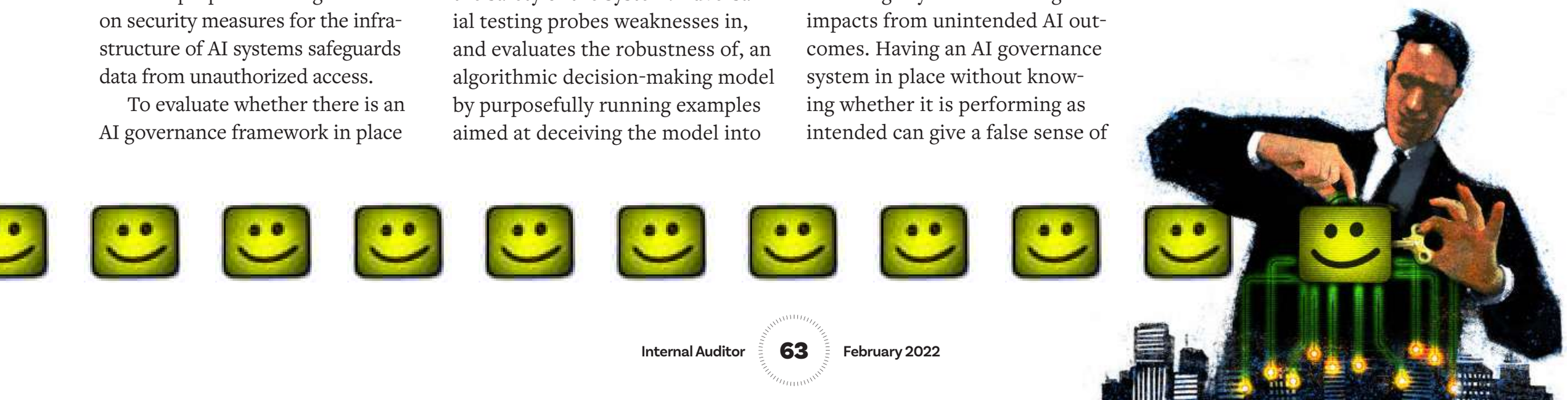
Continuous Independent and Objective Review

Putting AI governance in place is only the first step. It is essential to verify that it is working appropriately and to enable improvement over time. If the AI governance framework is not evaluated, it could even magnify the risk of negative impacts from unintended AI outcomes. Having an AI governance system in place without knowing whether it is performing as intended can give a false sense of self-assurance, decreasing vigilance and preparedness.

The objectives of an audit might include the effectiveness and efficiency of the AI system, the reliability of using the information generated by the system, and compliance with applicable laws and regulations. Internal auditors are key to objectively evaluating AI governance, while avoiding conflicts of interest, by ensuring independence from the developers and users of AI systems.

Kitty Kay Chan, PHD, is professor of practice in Applied Analytics, affiliated member at the Data Science Institute, and academic director of the Master of Science in Applied Analytics at Columbia University in New York.

Tina Kim, CIA, CRMA, CISA, CPA, is deputy comptroller for State Government Accountability, New York State Office of the State Comptroller, in Albany.



boardroom

Welcome to the Talent Crisis

In today's business climate, talent management has become a strategic issue.

Matt Kelly

Executives often stress the importance of talent management for an organization's long-term success. Board directors, however, might soon find that they need to spend even more time worrying about it — because like so much else these days, talent is in short supply.

The headline of that idea is captured in the "Great Resignation": Employees quitting in record numbers, month after month. Right off the bat, the short-term disruption of those exits complicates an organization's pursuit of its long-term objectives. But there's more afoot here.

First, corporate cultures are undergoing profound transformation, thanks to COVID-19 and the shift to hybrid work environments, and increased emphasis on diversity, and heightened attention to workplace harassment. All of those forces are changing what employees want from their employer, and what makes an employee successful.

Second, it seems increasingly likely that today's temporary labor shortage is not temporary. A world chronically running short on talent would pose

strategic challenges that many boards haven't had to confront in a long time.

So how should a board think about talent management in that environment? Exactly what is the board's oversight role when hiring and employee retention are primarily management's responsibility? How can boards fulfill those duties successfully?

Defining the Board's Role

First we should clarify the board's role in hiring versus its role in talent management. The board hires the CEO and grooms other senior executives as part of CEO succession planning — but that's typically all the direct personnel oversight a board does. It would not, for example, set hiring targets or determine compensation levels for employees.

Instead, boards are there to review talent management proposals brought to them by the CEO: hiring plans for the upcoming year, equity compensation programs, or reorganization plans. The board is there to assure that management's plans for cultivating talent make sense and support the organization's overall business strategies.

The question of the moment, then: How does management plan to respond to the "Great Resignation," the push for more diversity, the hybrid work environment, and related pressures, so the organization can maintain the talent it needs?

Make no mistake, those pressures are daunting. Here are some statistics to leave you unsettled:

- According to the U.S. Bureau of Labor Statistics, the number of people quitting their jobs in the U.S. went from 3.3 million in September 2020 to a record 4.4 million in September 2021 — an increase of 34%.
- In the U.K., a survey of 6,000 workers by recruiting firm Randstad found that 24% of employees planned to quit in the next year.
- The Microsoft 2021 Work Trend Index, a survey of more than 30,000 workers worldwide, found that 41% were considering resigning or changing professions in the coming year.

A world running chronically short on talent would pose strategic challenges that many boards haven't had to confront in a long time.

Such instability can have enormous implications for businesses: higher compensation costs, revenue shortfalls because of labor shortages, and more operational mistakes from newly hired employees. Insufficient labor and talent might even force a company to change strategies, perhaps scrapping new

product lines or outsourcing projects that might otherwise be handled in-house.

That's the real issue here. In today's economy — dominated by service-oriented businesses, powered by human capital, filled with a highly diverse workforce unafraid to part ways with an organization that doesn't meet their standards — the board can't simply shrug off labor instability and say, "Well, hire fresh people." All the company's ambitions could unravel during that time. Talent management has become a strategic issue, where the board needs to assure that the CEO is keeping pace with the challenge.

Most board directors already grasp that point in the abstract. The "Great Resignation" and related pressures just bring it into alarmingly sharp relief.

Building Better Oversight Mechanisms

If the board's job is to ensure that talent management supports the organization's overall strategy, the place to start is the board's relationship with the CEO. The board needs to set talent management objectives and make sure the CEO (and his or her management team) can achieve them.

The board can define those talent management objectives in several ways. First, the board can define objectives to ensure that promising senior and mid-level executives move into higher leadership roles. For example:

- Ask the CEO to propose a CEO succession plan.
- Set goals for the CEO to diversify the management team.
- Ask other senior executives to make presentations to the board, or even assign special projects to them.

Second, the board can define metrics for talent management at the middle and lower levels of the organization and then monitor progress toward those goals. Here, the board might track metrics such as employee turnover (by location, gender, employee level, and other criteria, if possible). It could ask for data about compensation rates compared to peer firms or about "employee net promoter scores," which measure employees' loyalty to the business.

Third, the board can monitor perceptions of its corporate culture and ask whether those perceptions might jeopardize hiring and retention. For example, how does data from employee satisfaction surveys trend over time? How do consumers perceive the organization, especially on issues such as diversity and climate change?

Whatever the answers to all those questions might be, boards then need to take the discussion further. Do those answers suggest a problem with talent management? If so, how could those problems challenge the company's ability to hit financial targets or achieve other objectives? And how does the CEO plan to address that?

Boards also need to consider which committee, if any, should take the lead on talent management. A larger board with a dedicated risk committee could assign the responsibility there. A governance and nominating committee might also fit, particularly for tasks related to CEO succession. Then again, as success at talent management becomes more important strategically, perhaps the whole board could ask about talent management as it reviews and debates strategy.

Internal Audit's Role

Given the rising importance of talent management, plus emerging pressures such as the "Great Resignation," internal audit can assist the board in numerous ways. As always, the goal is to provide the board with objective, reliable information about risks to the organization. In that case, internal audit could:

- Compile data, reports, or even dashboards to provide the board with a deeper, ongoing view into talent management issues across the enterprise.
- Conduct specific audits of, say, the human resources function, diversity programs, recruitment efforts, or CEO succession planning; where the audit team interviews employees to get "from the front lines" feedback about how they feel about the organization.
- Provide an analysis of how much strategic or operational goals depend on talent, and conduct scenario planning of what might go wrong if talent objectives aren't met.

Management always likes to say that the organization's people are its most important asset. The "Great Resignation" and so much else is putting that statement to the test. Boards will need to act deftly to ensure that their organization can pass it.

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

David Salierno

The bots are coming, but not from where you'd expect.

When it comes to innovation and high technology, most people think of places such as Tokyo, Tel Aviv, and Austin, Texas, where ambitious startups have developed reputations for disrupting industries.

Or perhaps Silicon Valley comes to mind, home to several of the most transformative social media and software companies on the planet. But sometimes, big technology ideas come from unexpected places.

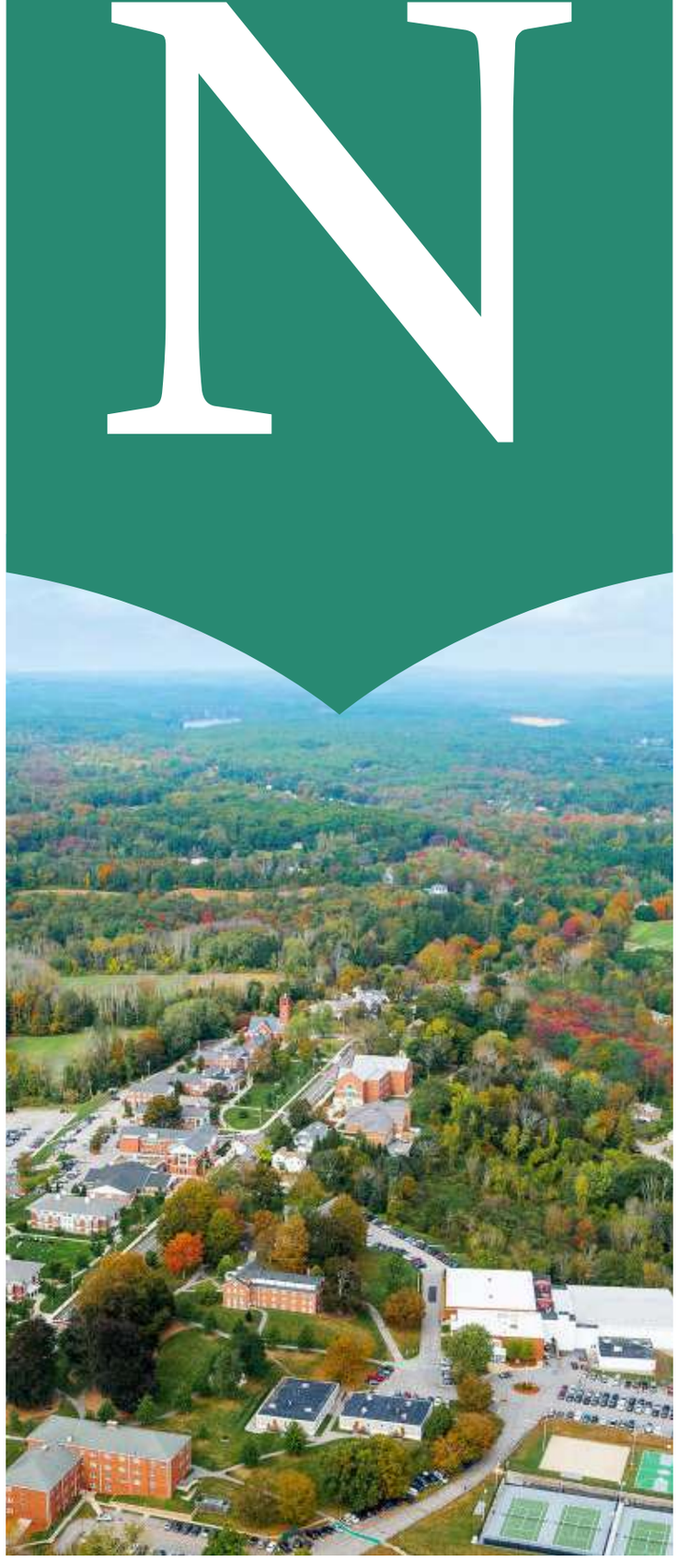
Take Nichols College, a specialty business school with an undergraduate enrollment of fewer than 1,200 students. In 2020, the college established its Center for Intelligent Process Automation (CIPA), an education and research facility aimed at training students to use robotic process automation (RPA). Located in the small town of Dudley, Mass., the facility is hardly situated in what most people would think of as a hub of technological innovation. And yet, the center provides exactly the type of hands-on skills that many of today's cutting-edge organizations expect from new hires.

What's more, the center serves as a community resource, helping businesses and professionals get up to speed on RPA and implement it in their organizations. It's also setting a clear example for others on how to embrace the technology.

"Our mission is to be a showcase," explains Bryant Richards, CIPA director and associate professor of Accounting and Finance at Nichols College. "It's as if to say, 'See, business students can be trained to analyze, build, and deploy automations — and if this plucky little school in Dudley can start their digital transformation, why can't other organizations?'"

Apprenticeship in Automation

The Center's origins can be traced to discussions several years ago with the Nichols Board of Trustees. One board member, retired investment executive Robert Kuppenheimer, shared emerging trends he was seeing in business — and their likely impact — and described how the school could leverage them.



CIPA officially opened in January 2021 and has trained more than 60 students in RPA fundamentals. Another 300-plus students have started the program, including nine participants in a graduate-level pilot. Among its enrollees, the center currently boasts six intelligent process automation analysts (IPAAs) — student experts who have been trained through the facility and now work as CIPA employees. "Our goal is to eventually be a 100% student-run center, though currently our faculty and IT staff provide support and guidance," Richards says.

In addition to their analysis and automation work for Nichols, the IPAAs work with businesses to help identify RPA opportunities and analyze processes, gaining experience that goes well beyond the classroom. For example, CIPA's student experts provided RPA assistance to Mohegan Sun, a casino and resort in Uncasville, Conn., where Richards formerly served as head of internal audit. The casino's auditors were looking to push the envelope with technology, Richards says, so he approached them about incorporating automation into their repertoire of tools. CIPA advised on training, support, and software, and it worked with internal audit to identify relevant use cases.

With CIPA's assistance, the audit function created a coded script, or bot, for casino tenant reviews, reducing completion time from about

40 hours to just seven minutes. The center also helped whittle a nearly 100-hour physical security audit process down to less than half an hour. "Mohegan has built use cases for both these automations and should be well on its way toward return on investment," Richards says.

This engagement is typical of the Center's work, he adds. Richards and the IPAAs have trained several organizations and helped them build RPA proofs of concept. In many cases, they're helping construct automations that the business has wanted to create but just hasn't had a chance to do.

It's Easier Than You Think

Despite the center's many successes so far, one barrier Richards sees to RPA learning and adoption is fear. In fact, he says a dominant theme with CIPA's instruction and consulting is uncertainty about the technology's level of complexity. "When I show students the dashboard tool we use, it doesn't look like anything they've ever worked with before, and there's new terminology to learn," he says.

But Richards says the apprehension students feel is short-lived. Once they begin using the software and realize the learning curve is nowhere near as daunting as they had expected, students become enthusiastic about what RPA can do.

The same is true for business users, whose concerns are more focused on whether the time invested will lead to a productive outcome. To alleviate that, Richards says he looks to move business users quickly to adding value. In fact, he says these

With CIPA's assistance, the audit function created a bot for casino tenant reviews that reduced completion time

FROM 40 HOURS TO 7 MINUTES

users can learn to code fairly advanced and complex automations with only a couple weeks' training. And after just a few months, they can begin deploying automations that return high value. That same learning curve applies to internal auditors.

"The profession is uniquely suited to be good at this, because auditors' skills map perfectly to the task," Richards says. "We're not telling them to be coders, programmers, or IT people. We're telling them to take some steps to learn a new tool because those steps are going to be super valuable — and the momentum will build from there."

Seeing the Possibilities

Richards says once students at the Center become comfortable with the technology and see its potential, their learning accelerates dramatically. As the process becomes less conceptual and more concrete, they start looking at data differently and seeing all kinds of possibilities. And that, he says, is a key takeaway for the audit profession.

"That's a powerful thing that needs to be part of our skill set in the future," he says. "Auditors are going to start jumping into the technology, experimenting with managing variables, and developing strategies about capturing the data and moving it around. If they haven't seen data clearly before, they'll see it very well through this technology."

As an example of RPA's eye-opening possibilities, Richards points to a collaboration between CIPA and a team of students within the college's Criminal Justice and Counterterrorism programs, led by Associate Dean Allison McDowell-Smith, with the U.S. Department of Homeland Security Center for Prevention Programs and Partnerships known as the CP3 Invent2Prevent project. CIPA, in consultation with the McCain Institute for International Leadership and Edventure Partners, recently developed and tested an RPA proof of concept for collecting Twitter data combined with human intelligence to identify misinformation online as it relates to targeted violence.

"Criminal justice and counterterrorism students must be able to use emerging technologies in combination with human intelligence to prepare for their future careers," McDowell-Smith says. "This project was a great opportunity for students to experience the challenges and opportunities of including RPA as part of their methodology."

"If they haven't seen data clearly before, ***they'll see it very well through this technology.***"

—Bryant Richards, CIPA director, associate professor of accounting and finance, Nichols College

Bring on the Bots

Richards admits that counterintelligence was an application he had never thought of, but it's an example of how once users delve into the technology and start asking questions about its capabilities, horizons broaden and new possibilities begin to emerge. What excites Richards about the future of RPA is the enormous potential for transformative change and improvement. "We will see innovation in internal audit like we've never seen before," he says.

But no one can reap the benefits of automation without first taking the plunge — and Richards insists that the technology is within everyone's reach. "You've got to experience it firsthand, and when you do, the value becomes crystal clear," he says.

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

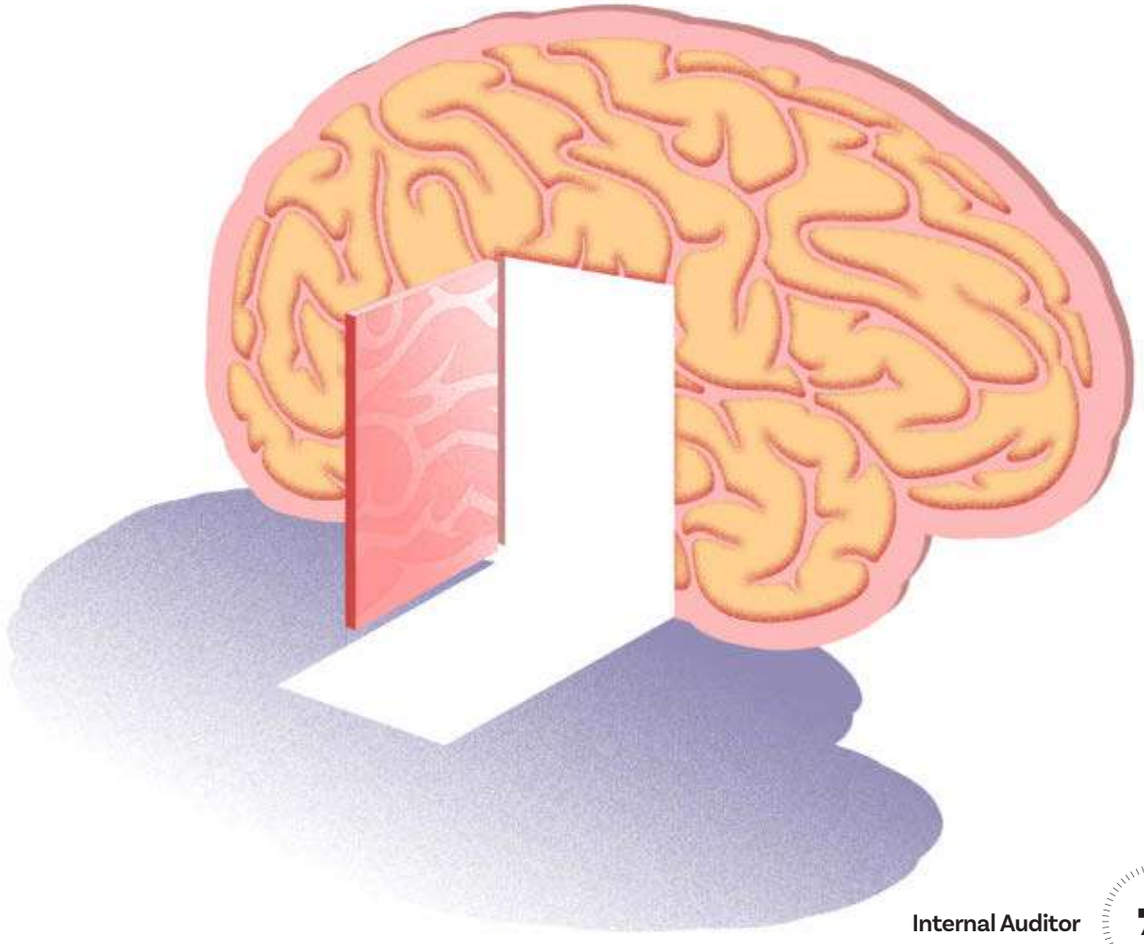
viewpoints

Psychological Safety in the Workplace

Employees who feel safe are more likely to speak up and question the status quo.

Joshua Clark

Margaret Belden
HR Transformation Director
Grant Thornton LLP



What does an organization that is psychologically safe look like?

Psychological safety can look and feel different to many individuals. That said, there are some core tenets that are common in a psychologically safe environment. First is the ability to feel comfortable speaking up, sharing ideas, expressing concerns, providing a contrary opinion, making mistakes, or offering feedback. Second, psychological safety means the people in these settings — no matter their level, role, or skills — will not judge, dismiss, or make another individual uncomfortable for speaking up. Finally, leaders in a psychologically safe environment reinforce expectations through actions and shared standards. This may mean rewarding employees who contribute to a safe environment or addressing actions that hinder a team's psychological safety. It could even mean pulling someone aside and calling it out when someone disrupts the psychological safety of another.

Are there certain groups that struggle more with psychological safety in the workplace?

There are several groups of people who struggle more with psychological safety. One group is junior or less-experienced staff. These employees generally feel more threatened to speak up for fear of losing a job or being labeled a "troublemaker." Another vulnerable group are employees from different cultures where the norms of what is and is not appropriate in a work setting may conflict with the ideals of a psychologically safe environment. A third group are employees who are fearful of losing their positions if they speak out or challenge the organization. Traditional organizational hierarchies have conveyed a chain of command that, at times, may prevent escalation of issues, while the lack of cultural awareness can limit the ability to create safe environments.

What actions can leaders take to promote inclusion?

First, the organization's leaders must determine whether they have an inclusive organization. Then, in partnership with human resources (HR), the diversity, equity, and inclusion team should educate leaders on what an inclusive environment consists of and enlist their support and understanding. It's also vital to celebrate and connect the importance of inclusivity to the business. This can be done in partnership with the CFO and the sales division by illustrating client expectations and providing data that shows how inclusive cultures increase profitability. The organization should set clear goals and expectations for what employees can expect — and put those goals into action. HR should also survey and, more importantly, listen to employees and ask the tough questions to determine if the organization is inclusive. Evaluate every aspect of how teams operate and analyze how meetings are set up; take a close look at who regularly contributes. Another area to look at is talent management, including acquisition, development, onboarding, advancement, rewards, and retention. Who is benefiting the most in these settings? Who is driving the decisions? Are the same individuals recommended for new assignments or projects time and again, and is the selection criteria broad or narrow? Finally, hold everyone within the organization accountable, as inclusion happens throughout the work cycle and in every single interaction.

"Another area to look at is talent management, including acquisiton, development, onboarding, advancement, rewards, and retention. ***Who is benefitting the most in these settings? Who is driving the decisions?***"

—**Margaret Belden**

Sarah Fedele
Internal Audit Leader of U.S. Risk & Financial Advisory, Deloitte

In today's business climate, why is it important for organizations to have psychological safety in the workplace?

Most organizations have experienced extraordinary change, from pandemic-driven remote work, to talent turnover, to structural shifts. As a result, many individuals are now serving in new roles or organizations. So much individual and organizational change may leave some employees feeling less psychologically safe than they have in years. Yet psychological safety is key to team performance and more essential than ever during ongoing pandemic-driven disruptions. If individuals don't feel safe enough to do things like ask for help, admit mistakes, or critically assess team performance, risk management can become fraught with new and more complex challenges. For internal auditors personally, the pressure remains very much "on." In a 2020 Deloitte global survey, we found that 96% of audit committee members expect the demands on internal audit's skill set to increase in the next three to five years. Now is the time for

CAEs to focus on establishing psychological safety on their own teams, harnessing their collective power, and leading them to high performance.

Why is psychological safety difficult to maintain?

As with most cultural matters, leaders set the tone for creating and respecting psychological safety within teams. Teams need to embrace the mindset that everyone is doing the best job they can, given what they know, their skills and abilities, the resources available, and the situation at hand — and commit to constantly improving based on learnings. It takes a lot of people acting congruously to build and maintain a psychologically safe environment, which can be a real challenge.

Of course, organizations that create and maintain cultures of psychological safety realize great results in terms of improving transparency, accelerating collective learning, and enhancing overall team performance. When psychological safety is achieved, it can be an invaluable boon to organizational culture.

How can internal auditors measure an organization's level of psychological safety?

Internal audit teams can assess an organization's level of psychological safety by looking at how leadership does or does not humanize itself by taking ownership of failures; how organizations recognize or reward actions that support psychological safety; and how teams leverage continuous improvement frameworks like Agile into the mainstream narrative of the function. Further, internal audit teams can help organizations hone their psychological safety levels by suggesting a shift in behavior or new ways of working. Team-level coaching can be particularly helpful, as it focuses on the behavior and dynamic between team members to support stronger psychological safety, intent-based leadership, and continuous improvement.

More specifically, internal audit teams could consider asking questions to begin assessing organizational psychological safety and their role in promoting it. For example: Does the organization work to develop an atmosphere of trust, a culture of sharing views, and an acceptance of constructive criticism? Can audit reports focus on improvements that can be made, recognizing what went wrong but emphasizing what can be learned from those events? Does internal audit leadership work closely with management, especially the CEO and CFO, and can the team help educate management on the key risks and controls to improve mitigation and management? And finally, can internal audit help develop incentives for management to identify and communicate the need for controls improvement opportunities, anomalies, or new risk drivers — without fear of retaliation or unfavorable consequences?

> Teams need to embrace the mindset that everyone is doing the best job they can given what they know, their skills and abilities, the resources available, and the situation at hand — ***and commit to constantly improving based on learnings.***
>
> —Sarah Fedele

Grappling With the *Fatigue Factor*

Third Annual American Corporate Governance Index

While the overall ACGI score held at a B-, the same as in 2020, the strength of the nation's corporate governance has been tested by prolonged pandemic pressures and there are areas that are showing the strain. See what's holding strong and what might be cause for concern by getting your copy of the 2021 American Corporate Governance Index.

Strengthen your knowledge of American corporate governance. *www.theiia.org/ACGI*

The Institute of
Internal Auditors
Elevating Impact

2021-3857

IAm

Dominique Vincenti

When I was growing up, I wanted to be an astronaut, a symphony orchestra conductor, a comedian/actress, a spy, an ambassador, a dancer, a writer, a chef, a magician, a president, a resort manager, a historian, a rock/pop singer, an Olympic swimmer, and an airline station manager, all at the same time, and I still do. Thank God I found internal auditing, which for nearly 30 years now has allowed me to quench my thirst for adventure, curiosity, diversity, creativity, innovation, fun, and leadership, and have the most extraordinary human encounters and experiences from the mailroom to the boardroom around the world.

Do not ask me what my preferred book, my preferred food, my preferred film, my favorite game, my favorite sports, or my preferred music is. I hate to be forced to choose — and why should I? I love it all, and I cultivate it all.

My fuel: the unconditional love of my parents, of my in-laws, and of my extraordinary husband. "Ma raison de vivre" and who I would die for: my children, Ana and Nathan.

stats

Uber
CIA, CRMA

Vice President, Internal Audit

IIA Member since 1994
San Francisco Chapter