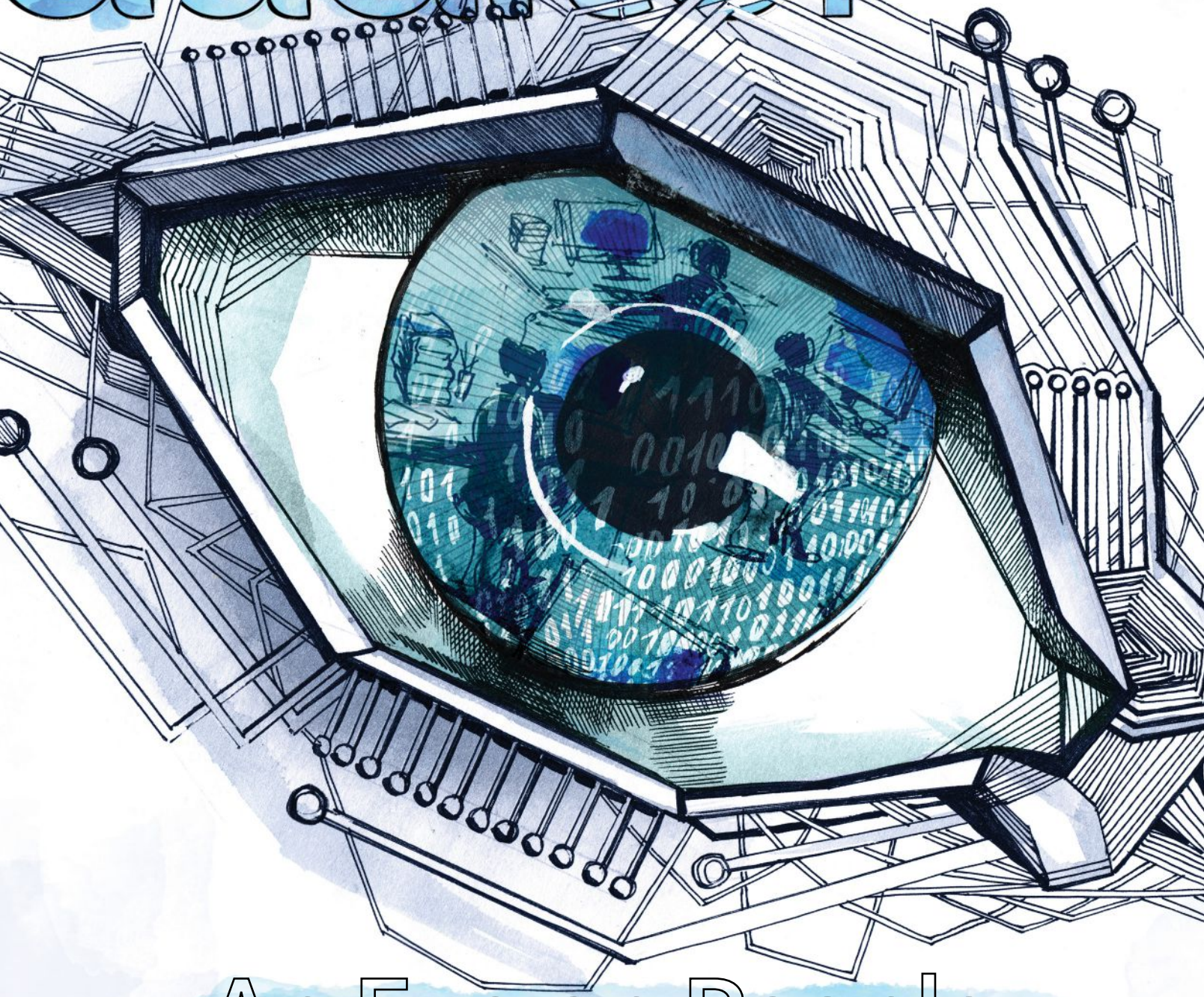
Risk Focused. Future Ready.
New IIA Global Chair shares her priorities

Upping the Board's Game
Internal audit's advice strengthens oversight

internal auditor

AUGUST 2026
A PUBLICATION OF THE IIA



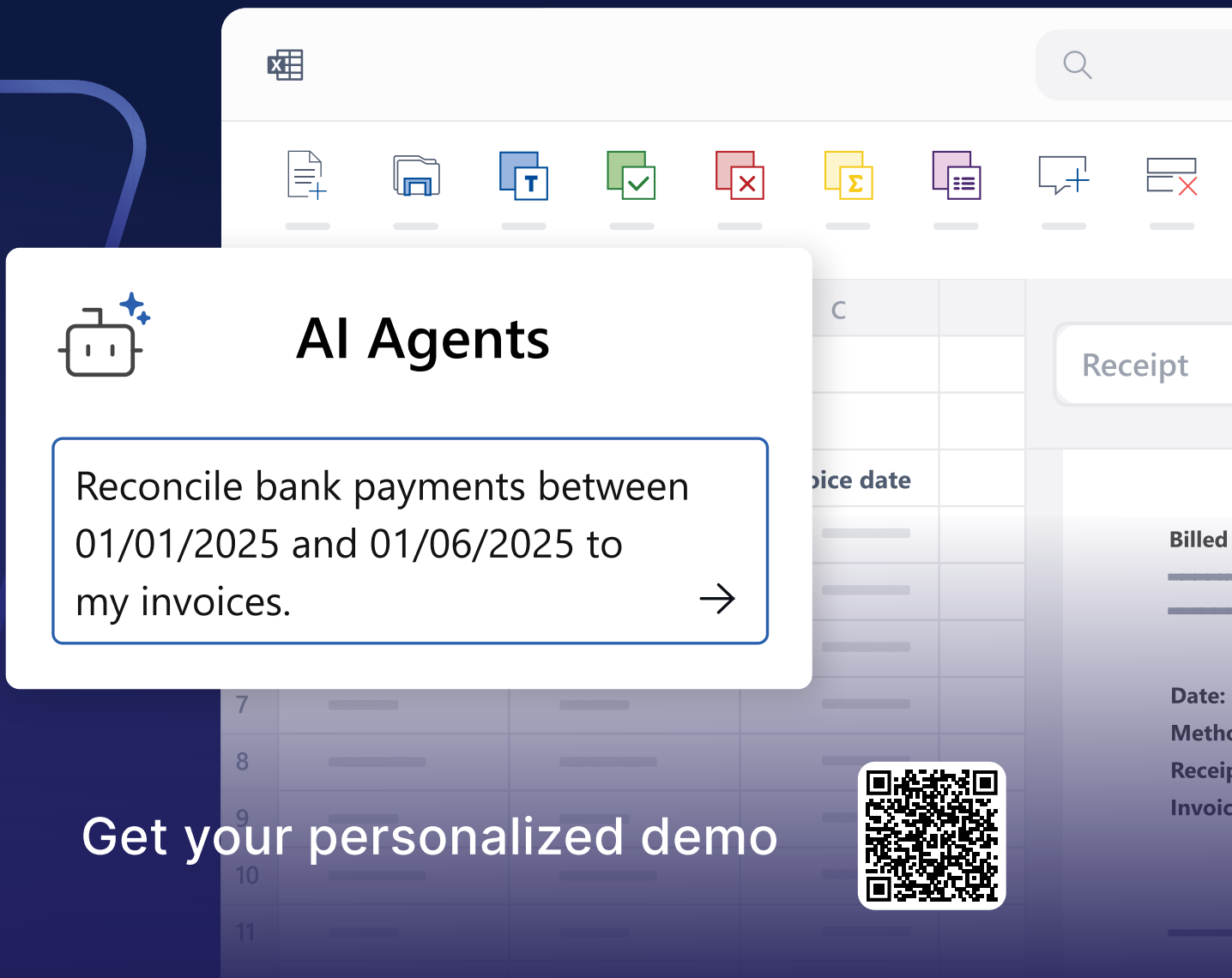
An Eye on People

Human capital risk in an AI world.

datasnipper

Turn complex testing into confident decisions.

Let AI Agents handle the heavy lifting inside Excel.



Get your personalized demo

IGNITE

2026 • CONFERENCE

Where Internal Audit Leaders Emerge

Accelerating leadership impact

Discover actionable insights, innovative strategies, and invaluable connections that help you navigate today's evolving risk landscape — and lead with greater confidence tomorrow.

November 2–3, 2026
Washington, DC & Virtual

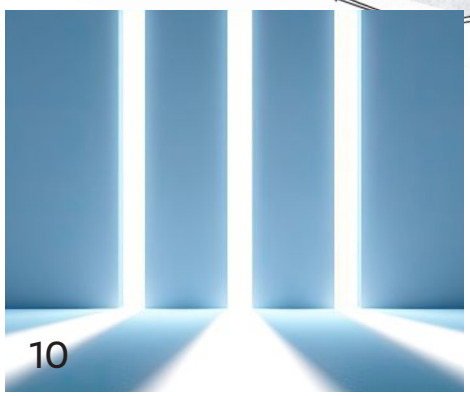
REGISTER TODAY! • ***theiia.org/IGNITE***

IIA

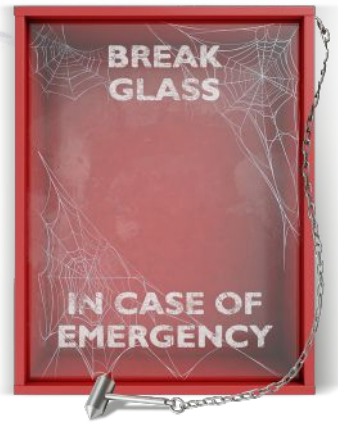
contents

featuring

22



10



18

departments

54

60

Start Here

Show employers you're serious about pursuing internal audit proficiency with the Internal Audit Practitioner™ (IAP™).

A globally recognized credential that puts you one step closer to earning the Certified Internal Auditor® (CIA®).

Get started now at theiia.org/IAP

IAP™
Internal Audit Practitioner™

CE message

Opening Doors to Internal Auditing

As students prepare to begin a new school year, I'm inspired by the momentum building across The IIA and the Internal Audit Foundation to strengthen the future of our profession. That momentum is especially important because earlier this year, the Foundation's Preparing for the Next Generation of Internal Audit Talent report highlighted a significant awareness gap. Nearly half of the students surveyed globally don't understand what internal auditing is and have never considered it as a career.

At the same time, Vision 2035 survey respondents say entry-level internal auditors will need the more advanced capabilities that Gen Z — and soon Gen Alpha — is already bringing to the workforce such as digital fluency and strategic thinking. Our responsibility is to ensure they see internal auditing as a profession where their skills and strengths can thrive. To support that goal, The IIA offers complimentary global student membership to help more students explore the profession.

Today, we're taking another important step by launching DoMoreWithInternalAudit.com, a website that introduces students and emerging professionals to the possibilities of a career in internal auditing. Built around the theme "Internal Auditors Do More," the platform helps students learn about the profession's career opportunities, growth and earning potential, and the critical thinking skills that enable organizations to succeed.

This initiative is part of a broader global effort to strengthen the profession's talent pipeline. This past year, the Foundation awarded more than $278,000 in grants and scholarships. Universities enrolled in the Internal Audit Academic Alliance Program are eligible for scholarships and grants through the Foundation, helping institutions integrate internal audit education into their curriculum and prepare future practitioners. To date, The IIA has endorsed 181 universities across 43 countries, including 16 new institutions in 2026.

In line with these efforts, we are also seeing growing enthusiasm among students. This year's Global Student Conference in Orlando, Fla. welcomed 223 attendees from 19 countries. In the coming months, a new Foundation webinar series will enable students to learn directly from professionals and explore internship opportunities.

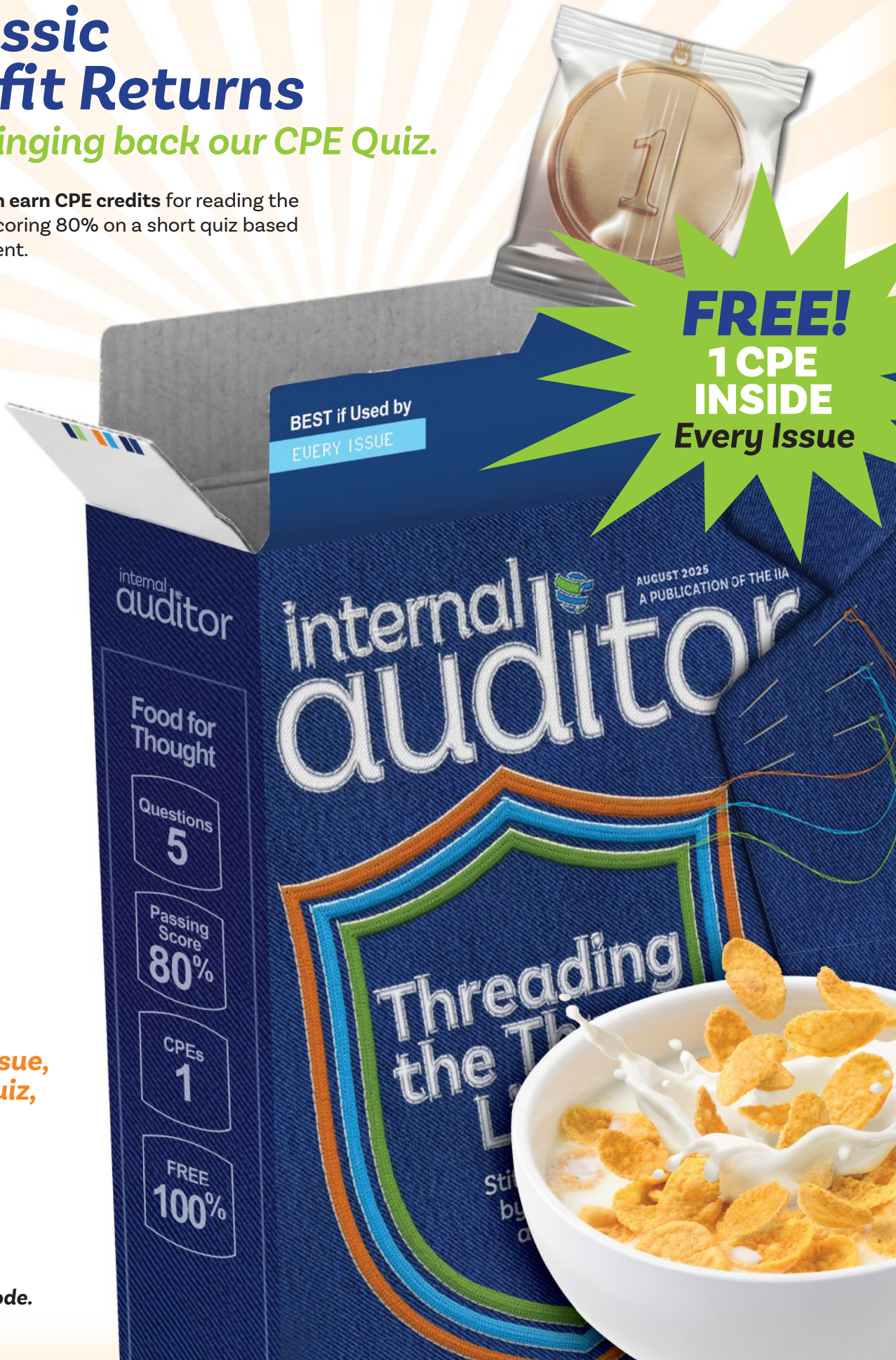
The future of internal auditing depends not only on how we adapt to and respond to change, but on how effectively we inspire the next generation to join us. By investing in awareness, education, and opportunity today, The IIA is helping ensure the profession remains strong, innovative, and relevant for decades to come.

Anthony Pugliese

A Classic Benefit Returns

We're bringing back our CPE Quiz.

IIA members can earn CPE credits for reading the magazine and scoring 80% on a short quiz based on feature content.



Read the Issue, Take the Quiz, Earn 1 CPE.

Scan the QR Code.

editor's note

People and Avatars

"That seems very impersonal," I thought when I heard the news that Meta was developing an artificial intelligence (AI) avatar of its CEO, Mark Zuckerberg, to interact with the company's employees. But that first impression altered a little when I interviewed Career Nomad CEO Patrice Williams-Lindo for the video accompanying this issue's "The Big Idea" (page 57). Williams-Lindo says these executive digital twins are going to be a big thing.

Executive avatars are one of the more visible ways in which AI and people are intersecting in modern businesses. Whether it's how AI will impact the availability of jobs or how it is changing how work is performed, the common thread is people.

Our August cover story, "Human Capital Risk in an AI World" (page 22), explores how AI is impacting human capital risk. Organizations can use AI to address human risks related to customer relationships, fraud, physical safety, and workplace bullying, write Thomas Diamonte, Richard Chan, and Manuel London. AI's analytical abilities also enable it to uncover cultural issues and organizational dynamics that can impact performance.

But there is a dark side. Those same AI capabilities can increase human capital risk if they initiate a surveillance culture that harms morale and leads to distrust and staff turnover. In assessing AI's use in workforce management, internal auditors should look for a balance between employee trust and data governance, the authors say.

Governance is crucial for those people-facing executive avatars, too, Williams-Lindo notes. It provides guardrails to ensure there is trust, credibility, and stability — without those three things the technology fails. If the communication is important and consequential, it should come from the real CEO, she warns. "When employees can't distinguish between a human decision and a machine simulation of one, you don't just have an engagement problem — you have a governance exposure," she says.

In "The Big Idea," Williams-Lindo explains how executive avatars are already appearing in earnings calls, and Zuckerberg is just one of the many CEOs who see their potential. With appropriate governance, an avatar could extend the CEO's vision and reach in ways one individual could not accomplish, she says.

Like I said, Williams-Lindo has convinced me that executive avatars are going to be huge. Maybe I should get one.

TimMcCollum10

internal auditor
AUGUST 2026

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.

A PUBLICATION OF

The Institute of Internal Auditors

PRESIDENT AND CEO
Anthony Pugliese, CIA, CPA, CGMA, CITP

CHAIR OF THE BOARD
Stacey Schabel, CIA, CPA

CHALLENGE Yourself

One streamlined exam for qualified professionals. One globally recognized certification.

Earn the world's only globally recognized internal audit certification through the one-part CIA Challenge Exam. Perfect for eligible accounting professionals, CISA™ holders, and seasoned internal auditors. The Certified Internal Auditor® (CIA®) elevates your credibility and demonstrates your knowledge of the Global Internal Audit Standards™.

Check eligibility.

CISA™ is a trademark of ISACA®

CIA® Challenge Exam

update

New Perspectives on Three Lines and ERM

The IIA issues major updates to internal audit position statements.

The IIA recently updated two seminal position statements on the Three Lines Model and enterprise risk management (ERM) to reflect internal audit's growing role in advising the board and integrating assurance across functions. Now called Statements of Position, they communicate The Institute's views on these topics to organizations and the internal audit profession.

The refreshed Three Lines Model highlights the board's oversight role and clarifies the responsibilities of the first, second, and third lines by emphasizing the contributions of each to strong governance and risk management.

"This Statement of Position is essential reading for boards and senior leaders because it defines how assurance and advice should work together to provide the reliable, independent, and coordinated insights needed for effective governance in today's increasingly complex organizations," says Benito Ybarra, executive vice president, Global Standards, Guidance, and Certifications at The IIA.

The updated ERM statement, The Role of the Internal Audit Function in Enterprise Risk Management, defines ERM as a coordinated set of activities for identifying, assessing, managing, monitoring, and reporting risks. It replaces the longstanding ERM "fan" diagram with a new model that depicts how the five categories of ERM activities connect to the internal audit function's assurance, advisory, and administrative activities. The diagram makes clear that decision-making remains management's responsibility.

"Internal audit delivers its greatest value by combining independent assurance with trusted advice, helping boards and management strengthen decision-making, while preserving the independence that defines the profession," notes Katleen Seeuws, IIA vice president, Standards and Guidance.

These papers are the first in a series of updated Statements of Position, with more planned for 2027. Endorsed by The IIA's Global Board of Directors, the statements aim to help boards, audit committees, and executives make informed decisions on accountability, oversight, and organizational performance.

Both statements are available online at theiia.org/sop. *—Lauressa Nelson*

FROM WORK TO HOME

Workplace AI tools drive consumer use.

78%

of AI users choose employer-provided AI tools for personal use.

27%

of U.S. consumers use AI for work and daily life.

SOURCE: PYMNTS INTELLIGENCE, THE CONSUMER AI BENCHMARK REPORT

Bad Actors Earn Trust With AI

Cybercriminals create more targeted and sophisticated social engineering scams.

The FBI recently warned that the Silent Ransom Group criminal gang is using a variety of tactics to steal data from U.S. law firms and banks. Their methods include social engineering, vishing, and phishing — impersonating IT support personnel via a direct call or sending convincing emails to urge employees to call them.

Once on the phone, the gang directs employees to grant remote access to their computers or download programs that provide attackers ongoing control. In some cases, gang members even showed up to organizations in person to physically insert hard drives into a victim's computer.

Tactics such as impersonation, social engineering, and compromised credentials are driving a rise in fraud attempts and losses at financial institutions, according to the U.S. Federal Reserve's 2026 Risk Officer Report. In a survey of 400 U.S. banks, 72% of respondents say cybersecurity is a persistent or increasing critical risk.

Of particular concern, AI-generated phishing and vishing is increasing, with AI detected in 86% of phishing emails, according to security and training firm KnowBe4's Phishing Threat Trends Report. Criminals can build highly convincing social engineering campaigns using AI prompts and information pulled from LinkedIn profiles, company websites, breached data, and even recordings of executives speaking on earnings calls and at conferences.

"Social engineering is becoming more targeted, making it more difficult to discern what is legitimate versus what is malicious," says Jack Chapman, senior vice president of Threat Intelligence at Clearwater Fla.-based KnowBe4 in a press release.

Like the Silent Ransom Group campaign, callback phishing, where victims are prompted to call the perpetrator, can create a false sense of security. This more personalized approach "allows the attackers to establish contact and maintain a rapport before delivering their malicious payload," KnowBe4's report notes. *—Christine Janesko*

COUNTING TIPS

An analysis of occupational fraud cases shows how whistleblower hotlines pay off.

43%
OF FRAUDS
are detected by tips.

55%
OF TIPS
come from employees.

1/3
OF TIPS
come from customers and vendors.

SOURCE: ASSOCIATION OF CERTIFIED FRAUD EXAMINERS, OCCUPATIONAL FRAUD 2026: A REPORT TO THE NATIONS

SEEKING COVER

In a study of insurance risks, the top three concerns among consumers, small-business owners, and insurance professionals in the U.S. and U.K. were:

- Cyber risks.
- Business interruption.
- Natural catastrophes — including floods, winter storms, and thunderstorms.

SOURCE: MUNICH RE US, RISKSCAN 2026: RE(INSURANCE)

ASK AN EXPERT

Safety First

Scott DeBow, CSP, ARM, is director of Health, Safety, and Environmental at Avetta, a supply chain risk management company, and an author for the Avetta Insights & Impact Report 2026. He is based in Atlanta.

What factors impact safety on job sites?

While minor workplace injuries have steadily declined, fatality rates are a different story. According to International Labour Organization data, nearly 3 million workers die from work-related accidents and illnesses globally each year. Fatality rates worldwide have plateaued.

The biggest exposures rarely live in documented, routine processes. They live at the edges and the "in-betweens" — in workarounds and shortcuts. Nonroutine work tasks carry disproportionate risk, as do scope changes that happen mid-task. When work shifts from planned to unplanned, controls designed for the original task may no longer apply.

Resource gaps are another factor. When staffing, equipment, or time are reduced, workers improvise, introducing risk that was never assessed.

How are organizations lowering risks?

Most companies manage safety as a compliance exercise, but compliance alone does not prevent fatalities. Leading organizations are moving beyond compliance toward an approach that is performance-based and built around key practices.

One method is to prioritize incidents by severity, not frequency. Traditional safety metrics count incidents. A better way is to weight them — distinguishing between a sprained wrist and a near-fatality. Severity-based lagging indicators provide richer context and stronger predictive value for preventing the most serious events.

Another practice involves mapping high-hazard activities and honestly assessing whether required safeguards are present, partial, or absent. Degraded or missing controls around lethal energy sources represent the most urgent exposure and should be addressed immediately.

Getting executives involved is another factor. When leadership takes an active interest in reducing serious incident and fatality risk, the entire organization orients around it, closing the gap between policy and practice.

Finally, asking "Where are we good?" versus "Where are we lucky?" is the most important mindset shift. Leading organizations don't just investigate actual incidents — they systematically review potential serious incident and fatality events to determine whether a serious outcome was avoided by design or by chance. A near-miss that no one examines is a fatality waiting to happen. Luck is not a control.

HACKS OVERTAKE SCAMS

In the U.S., hacking has surpassed scams as the leading cause of identity theft.

26%

of victims are now dealing with two or more identity incidents at once.

For adults ages 35–64,

UNAUTHORIZED DEVICE ACCESS

is now the leading cause of identity theft.

SOURCE: IDENTITY THEFT RESOURCE CENTER, 2026 TRENDS IN IDENTITY REPORT

The biggest exposures rarely live in documented, routine processes. They live at the edges and the "in-betweens" — in workarounds and shortcuts.

Expand Your GRC Insights

Set yourself up for success in the dynamic governance, risk and control environment with world-class content, innovative ideas and practical guidance. Plus, earn up to 28 CPE credits. Join The IIA and ISACA for the GRC Conference 2026 in sunny **San Diego, 17–19 August**.

GRC 2026 Conference

Scan QR code to learn more.

IIA | ISACA

Driving Audit Improvement

Internal audit increases its value by refining processes, perspectives, and professional development.

Alessandra Salazar

Internal audit is never static. It constantly evolves with changes in business environments, regulatory requirements, technology, and stakeholder expectations. These shifts require internal auditors to adapt their approaches, tools, and skills to better respond to risks.

A mindset of continuous improvement — focusing on process improvements, inviting diverse perspectives, and fostering ongoing education — helps internal audit strengthen organizational resilience and success. This mindset can shape how internal audit works, keeping it relevant and effective.

Identifying Process Improvements

There are many ways to make audits more efficient. Finding process improvements is not always easy and may require a review of the entire process. If auditors are stuck, they can gain a fresh perspective by bringing in a new auditor or one who does not usually work on that process.

When reviewing audit processes, internal auditors should identify manual steps, repetitive tasks, and opportunities to integrate technology. Internal audit should also assess if all steps involved in a process are necessary.

Process adjustments do not have to be groundbreaking; even incremental time savings are valuable. For example, a mid-sized U.S. financial services organization's internal audit function recently began using additional features in Microsoft Teams and Loop, a collaborative workspace app, to track audit statuses in a single space. This change streamlines collaboration and saves the team about 10 minutes a week during department meetings.

The bank's data science team develops, deploys, and monitors financial and statistical models. Recently, internal audit applied one of these models to a small quarterly audit, which previously comprised manual reviews that relied on reports from the core system housing all customer account information. Before the audit team began using the model, an auditor worked with the data science team to train the model and assess its accuracy.

Now that the model is in production, internal audit conducts this engagement quarterly, reviewing the model's outputs to verify accuracy. Once model training is completed, it should save the audit team about 20 hours per quarter, allowing practitioners to focus on more complex audits.

Preventing Groupthink

Diverse backgrounds can also strengthen internal audit. Having varied work experience, education, skills, thought processes, personalities, and cultures helps prevent groupthink by encouraging practitioners to evaluate facts instead of conforming to the views of the rest of the team. Different perspectives can produce better solutions, broader testing methods, and more thorough evaluations.

In a global environment, a diverse workforce also helps audit functions navigate different cultural norms. Internal audit should consider conducting a personality assessment to understand the team's strengths and weaknesses. The results can help the function identify gaps and set specific, measurable, achievable, relevant, and time-bound goals to address them. Different ways of thinking surfaces ideas teams might otherwise miss.

Asking for Feedback

Internal audit is independent, but it adds value by evaluating processes related to risk management, governance, and internal controls, while listening to stakeholder feedback and implementing appropriate changes. However, independence should not prevent the function from delivering meaningful results. Internal audit should ask itself: When was the last time we asked stakeholders what they wanted to see?

At the bank, internal audit learned that management does not have time to read the lengthy summary in the final audit reports. Senior management suggested adding an executive summary to each report — detailing a high-level overview. Since this change was implemented, senior management

has engaged more with the department's audit reports and offered better feedback.

Ongoing Education

Continuing education is critical for internal auditors and helps prevent complacency. Forty hours of training are required each year to maintain many relevant certifications and meet department standards, but the quality of that training matters. Internal auditors should consider webinars but also many other types of training, such as instructor-led courses, industry conferences, cross-functional job shadowing, and self-directed learning.

Auditors specializing in one area can strengthen their perspective by learning about adjacent disciplines, such as an operational auditor gaining exposure to data analytics or an IT auditor developing knowledge of fraud risk and investigation techniques.

Internal auditors should also step outside their comfort zones and learn about unfamiliar topics. By staying informed on emerging issues, such as artificial intelligence, cybersecurity threats, fintech partnerships, and evolving regulatory scrutiny, internal auditors can continuously adapt their approach and remain relevant.

Applying Improvement

Keeping internal audit aligned with business changes will protect its value and longevity. To avoid becoming obsolete, internal audit's relevance must evolve with the times. Auditors can practice this mindset today by evaluating their regular processes for areas of improvement.

During fieldwork, auditors should consider whether tests are as effective as possible. They should complete testing to identify overall strengths and weaknesses and ask stakeholders about audit pain points to save time and improve feedback. Adopting a mindset of continuous improvement can add immediate value to the organization and an auditor's professional life.

Internal audit should ask itself: When was the last time we asked stakeholders what they wanted to see?

Alessandra Salazar is an internal auditor at Capitol Federal Savings Bank based in Wichita, Kan.

Auditing Excel's Invisible Risks

Strengthening governance and controls can prevent spreadsheet errors from turning into costly problems.

Pratik Kalani

As organizations invest heavily in sophisticated enterprise resource planning systems and cutting-edge automation tools, a silent giant continues to dominate the business world: Microsoft Excel. Yet, using Excel without adequate controls introduces significant risk, as many models contain critical formulas that are vulnerable to accidental or unauthorized changes.

That overreliance can have serious consequences. In 2023, Norges Bank Investment Management, which runs Norway's Sovereign Wealth Fund, restated the fund's reporting after a single spreadsheet entry error caused a $92 million discrepancy.

To address this type of risk, internal audit should review Excel models with the same rigor it uses to audit core technology systems. Using a structured audit checklist and standardized observations can help organizations identify Excel's invisible risks, improve accountability, and support more reliable business decisions.

A Double-Edged Sword

Excel is widely used for data extraction, validation, analysis, and reporting. While speed and flexibility make it indispensable, organizations often underestimate its risks. Many organizations rely on spreadsheets for critical processes without putting controls in place to manage access, track changes, and verify the accuracy of data. That gap increases the risk of errors, unauthorized changes, compliance issues, and financial misstatements.

Excel's power lies in automating complex calculations with formulas and built-in functions, enabling dynamic models in which outputs update instantly as inputs change. These spreadsheets often embed customized logic and business rules. In effect, they are mini-systems where a change to a single cell can cascade across multiple calculations.

For example, a monthly payroll spreadsheet can automatically calculate salaries, taxes, and deductions with minimal input. While that automation is more efficient, it creates risk if formulas are incorrect or altered.

This reliance on Excel spreadsheets for critical business processes creates a governance gap that many organizations fail to recognize or address adequately: What if that formula changes? What if it's wrong? Who is checking it? What if accidental or unintentional changes are not detected quickly?

While enterprise systems are subject to formal controls, user-developed Excel models often are not. These models typically lack:

- ***Access controls.*** Users can share files freely without restrictions on who can view or modify them.
- ***Validation processes.*** Organizations don't formally verify formula accuracy and logic correctness.
- ***Change tracking.*** Models don't record modifications, making it impossible to trace the evolution of calculations or identify when changes or errors were introduced.
- ***Version management.*** Multiple versions circulate simultaneously, creating confusion and potential errors.
- ***Documentation standards.*** The business logic embedded in complex formulas is undocumented and understood only by their creators.

Excel's hidden risks sometimes surface during audit work. For example, during an engagement, internal auditors may come across risk-exposure models that have been built in Excel, with critical formulas unlocked and accessible to all users on a shared drive. Without

basic controls, unauthorized or accidental changes could materially distort risk assessments, expose the organization to compliance issues and financial losses, and destroy the audit trail.

An Excel Checklist

To address the significant risks posed by uncontrolled Excel usage, organizations need to have structured spreadsheet governance in place. This requires assessing how Excel is used and controlled, developing policies, implementing controls, and training users.

During audits, internal auditors can refer to a simple checklist to examine how Excel is used in high-risk areas, such as finance, inventory, procurement, and statutory reporting, or where standard Excel models are used more frequently. These audits should focus on four key areas:

- ***Security and Control.*** Auditors should evaluate the controls surrounding sensitive spreadsheets, including who can access and modify them. They should verify that access is limited to authorized users and that version controls help prevent unauthorized or accidental changes.
- ***Formula Accuracy.*** Formulas should be accurate, logically sound, and free from inappropriate hard-coding. Auditors can use Excel functions such as trace precedents and dependence to validate calculation flows.
- ***Data Integrity.*** Input cells should be clearly identified, subject to validation controls, and supported by reliable, documented data sources.
- ***Documentation and Oversight.*** Internal auditors should check that models are formally reviewed and approved, with documented change histories and clear ownership to support accountability and continuity.

When auditors identify spreadsheet control observations, they should translate them into practical remediation steps that address the root cause, reduce business risk, and assign clear ownership for follow-up (see "Spreadsheet Risks and Remedies" on this page).

To promote better governance, internal auditors can educate process owners about the inherent risks in uncontrolled spreadsheet use. They also can include Excel controls in risk control matrices and future walkthroughs.

Under Control

Recognizing and addressing spreadsheet risks can help organizations strengthen controls and reduce the potential for errors, compliance issues, and financial misstatements. For internal auditors, this is an opportunity to promote accountability and governance — but they must act before the next spreadsheet error becomes tomorrow's headline.

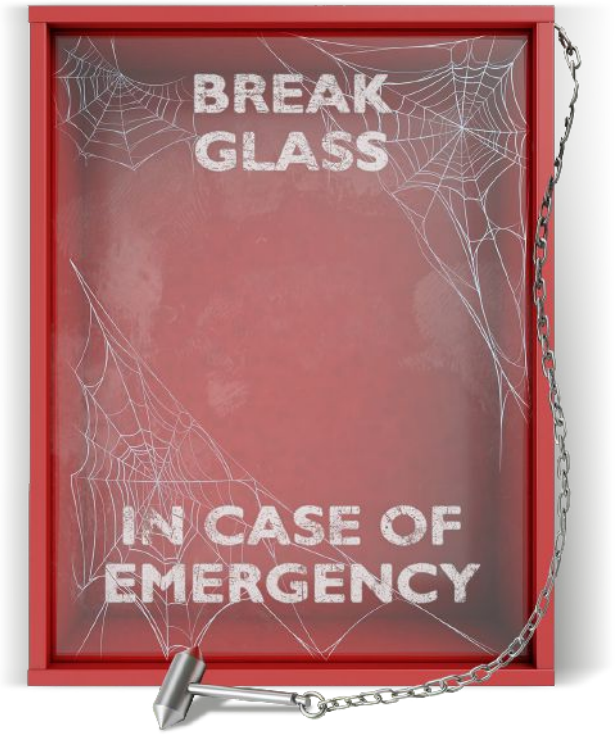
Pratik Kalani, CA, is a risk advisory professional with RAMA Group in Mumbai, India.

Spreadsheet Risks and Remedies

The table below outlines common spreadsheet control issues and what internal auditors can recommend to prevent them from impacting the organization.

Audit Observation	Root Cause	Potential Risk and Business Impact	Audit Recommendation
Critical spreadsheets lack formal validation or approval.	Excel models are not treated as governed systems.	Undetected errors may lead to incorrect decisions and financial misstatements.	Mandate peer review, approval, and periodic revalidation for critical spreadsheets.
Formula cells are unlocked and editable by all users.	There is no spreadsheet governance.	Unauthorized changes may distort calculations, risk assessments, and compliance.	Lock formula cells and restrict edit access to authorized users.
Changes to spreadsheet logic or formulas are not tracked.	User-developed models lack a change management process.	Errors cannot be traced, reducing accountability and detection.	Enable change tracking with formal approval and review.

Nobody's Decision



By tracing the governance of documented risks, internal auditors can avoid a decision risk gap, where no one is accountable for the exposure.

Pongpisit Wuttidittachotti and Pigulthong Kaewduangta

During an enterprise IT governance review meeting, senior executives paused over a risk dashboard summarizing cybersecurity vulnerabilities, third-party technology risks, and infrastructure resilience issues affecting a critical digital service. Despite the volume of analysis presented, no one in the room could confirm whether the organization had formally evaluated or accepted the overall exposure of that service. The discussion shifted from control effectiveness to a more fundamental question: Who was accountable for the decision?

When a service disruption later occurred, management could not demonstrate that residual risk had been explicitly accepted. Controls existed, but governance decisions did not. Budget constraints, accelerated digital transformation initiatives, and differing interpretations of risk tolerance contributed to the confusion.

Internal auditors frequently encounter such challenges: Risks may be recorded and monitored, yet decision accountability remains ambiguous. In such circumstances, the issue extends beyond control effectiveness to a broader governance gap in which risk information does not translate into accountable action.

The Decision Risk Gap

Traditional risk assessments focus on identifying threats, evaluating likelihood and impact, and recommending mitigation strategies. These activities implicitly assume organizations will ultimately make clear governance decisions about identified risks. In practice, this assumption does not always hold.

Organizations may maintain comprehensive risk registers and structured methodologies, yet documented risks do not necessarily lead to explicit decisions on how those exposures will be addressed. This gap can be described as decision risk — the risk that significant governance decisions are not clearly made, recorded, or owned.

Decision risk rarely arises from inadequate technical analysis. In many organizations, risk identification processes are methodical, structured, and supported by established frameworks.

The challenge instead lies in the translation of risk information into clear executive action. Documented risks may exist alongside uncertainty about who is responsible for deciding how the aggregated exposure arising from multiple individual risks should be addressed. As a result, governance processes can appear procedurally mature while still failing to produce accountable outcomes.

For internal auditors, recognizing this distinction is essential. They should assess the effectiveness of risk management not only by the quality of analysis, but also by the clarity of decision ownership and the visibility of governance responses.

Linking Information to Action

"The Decision Risk Traceability Model" on page 19 helps auditors trace decisions from the initial recognition of a risk, to the aggregation of exposure at the business-service level, to an explicit executive decision, to documented ownership of residual risk. At the business-service level, multiple individual risks are consolidated to reflect their combined strategic, operational, and regulatory impact.

Conceptually, it is easier to observe decision risk when diverse risk signals are consolidated to show exposure at the business-service level. For example, an internal audit identifies four independent issues affecting an online patient appointment system: delayed security patching, unsupported operating systems, incomplete backup testing, and dependence on a single cloud provider.

Individually, each issue is assigned a medium risk rating. However, when these risks are aggregated at the business-service level, executive management recognizes a significant risk of prolonged service disruption affecting patient care, regulatory compliance, and organizational reputation. The governance decision therefore shifts from evaluating isolated technical findings to determining whether the combined residual exposure is acceptable to the organization.

The defining governance moment is the explicit leadership decision — whether to accept, mitigate, transfer, or avoid aggregated exposure in light of strategic, operational, and regulatory consequences. Once exercised, decision authority establishes accountable residual risk ownership, which must remain subject to continuous monitoring and governance re-evaluation.

For internal auditors, tracing this end-to-end linkage provides critical assurance that risk governance is transparent, legitimate, and effective. By assessing whether this linkage functions effectively, auditors can move beyond verifying that risks are recorded and toward evaluating whether governance processes support timely, transparent decision-making. Where escalation pathways are informal or accountability is fragmented, organizations may face governance exposure even when technical controls appear adequate.

Making Ownership Visible

Decision risk carries broader implications for governance oversight. When accountability is unclear, audit committees may receive reports that describe risk levels but don't indicate who has formally assessed those exposures. Risk dashboards can become informational rather than enabling decisions.

Ambiguity in ownership can also weaken the application of risk appetite. Although policies define tolerance thresholds, they may have a limited effect on decision-making when authority at the operational or service levels is unclear. In complex digital environments, inconsistent decision-making may contribute to strategic misalignment and reduced transparency in assurance reporting.

To identify decision risk, internal auditors can extend their focus beyond control testing. Key considerations include whether:

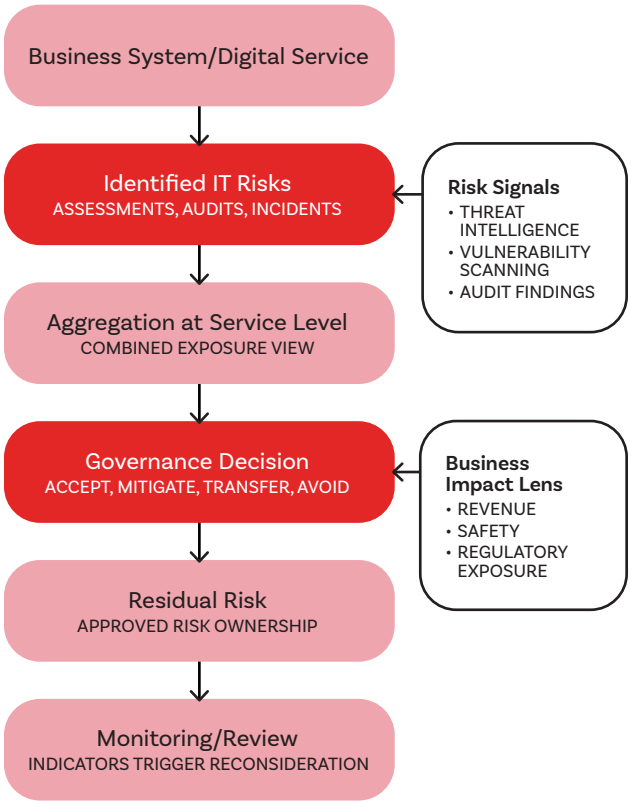
- Authority to accept aggregated risks is clearly defined.
- Governance decisions are documented.
- Mitigation aligns with executive priorities.
- Accountability remains visible if risks materialize.

The Future of Traceability

As organizations rely more on digital services and interconnected risk environments, strong risk management requires clear, timely decisions about how risks will be managed. By helping organizations trace who made those decisions, internal auditors can make risk reporting more credible, support more resilient strategic outcomes, and strengthen governance.

THE DECISION RISK TRACEABILITY MODEL

This model shows how diverse risk signals arising from assessments, incidents, or audit activities become meaningful only when combined into a business-service exposure perspective. Aggregation lets leaders evaluate overall business exposure rather than assessing individual risks in isolation.



Pongpisit Wuttidittachotti, PHD, CGRC, CISA, CGEIT, is cybersecurity and privacy officer at Huawei Technologies (Thailand) Co. Ltd., in Bangkok.

Pigulthong Kaewduangta, CISA, CISM, CRISC, CGEIT, is information security advisor at the Department of Health Service Support, Thailand Ministry of Public Health, in Bangkok.

Prescription for Fraud

A whistleblower lawsuit unravels the paper trail concealing a healthcare consulting firm's pharmacy kickback empire.

Joshua Clark

Pinnacle Health Advisors promoted itself as a problem-solver for the healthcare industry — a marketing and management consultancy that connected compounding pharmacies with physician networks. Co-founding brothers Elwood and Marcus Stanton had built the company from the ground up — alongside Elwood's wife, Renee, the vice president of finance, and his son, Derek. Together, the four controlled every critical decision at Pinnacle.

In late 2015, the Stanton brothers approached Robert Callahan, the owner of Meridian Rx, a small infusion pharmacy that was struggling to stay solvent. Their proposal was simple: Convert Meridian Rx from an infusion pharmacy that prepared medications for injection or intravenous use to a compounding pharmacy that prepared custom medications from raw ingredients. Meridian Rx would fill prescriptions generated through Pinnacle's physician network, with the two companies splitting the profits evenly.

The initial agreement explicitly excluded prescriptions covered by U.S. federal government healthcare programs such as Medicare, Medicaid, and TRICARE. These programs are covered by the U.S. Anti-Kickback Statute, which makes it a felony to receive payment for steering federally funded prescriptions to a particular pharmacy.

For a time, the scheme ran entirely on private-payer business, but the Stanton Brothers knew the real money was in federal programs. To expand the company's operations, Elwood directed Callahan to put Derek Stanton on the pharmacy's payroll. On paper, Derek was a Meridian Rx employee earning a modest base salary of $30,000 per year. In practice, he didn't report to anyone at the pharmacy or perform any duties there.

Instead, Derek received a 45% commission on every federal-program prescription that Pinnacle referred to Meridian Rx. The proceeds of that commission were funneled back to the other Pinnacle principals.

To track commissions internally without exposing the scheme's true nature, the conspirators devised a coding system. Prescriptions covered by government insurers were labeled with the prescribing physician's name followed by a "T," allowing the Stantons to calculate kickbacks owed, while concealing the paper trail. To receive and distribute the money, the group created a web of shell entities.

Beginning in late 2016, Pinnacle recruited a second pharmacy, Landmark Specialty Compounding. Under this agreement, the

kickbacks were disguised as fees paid to another newly formed entity, Crestview Partners, for purported "marketing services." In total, Pinnacle and the two pharmacies submitted claims of nearly $11 million to federal insurance programs and collected approximately $6 million in payments before the arrangement collapsed.

Pinnacle's scheme unraveled after Daniela Rourke, a commercial real estate broker whose former employer had previously done business with the company, sued under a provision of the U.S. False Claims Act. Rourke outlined the mechanics of the kickback scheme in granular detail.

The lawsuit triggered investigations by the FBI and the U.S. Department of Health and Human Services Office of Inspector General. Over the next few years, federal investigators gathered financial records, interviewed witnesses, and traced the movement of funds through shell entities. In 2021, a federal grand jury issued a criminal indictment against Pinnacle's principals and several co-conspirators at the pharmacies.

Each of the seven defendants pleaded guilty. Elwood Stanton, who directed the fraud, was sentenced to 36 months in prison and ordered to pay $4.2 million in restitution. Renee Stanton was sentenced to probation and the same amount in restitution. Marcus Stanton received a 15-month prison sentence, while Derek Stanton, the sham pharmacy employee, was sentenced to 14 months. The pharmacy owners received sentences ranging from 10 months to 14 months in prison.

The U.S. Attorney's Office also intervened in Rourke's civil lawsuit, adding the government's resources and reach to the False Claims Act allegations. That civil action ultimately produced more than $4 million in additional settlements and judgments.

The Pinnacle case shows how prescription kickback schemes are designed to evade detection by regulators. What ultimately brought the scheme down was a business associate who had access to information that regulators rarely see.

Lessons Learned

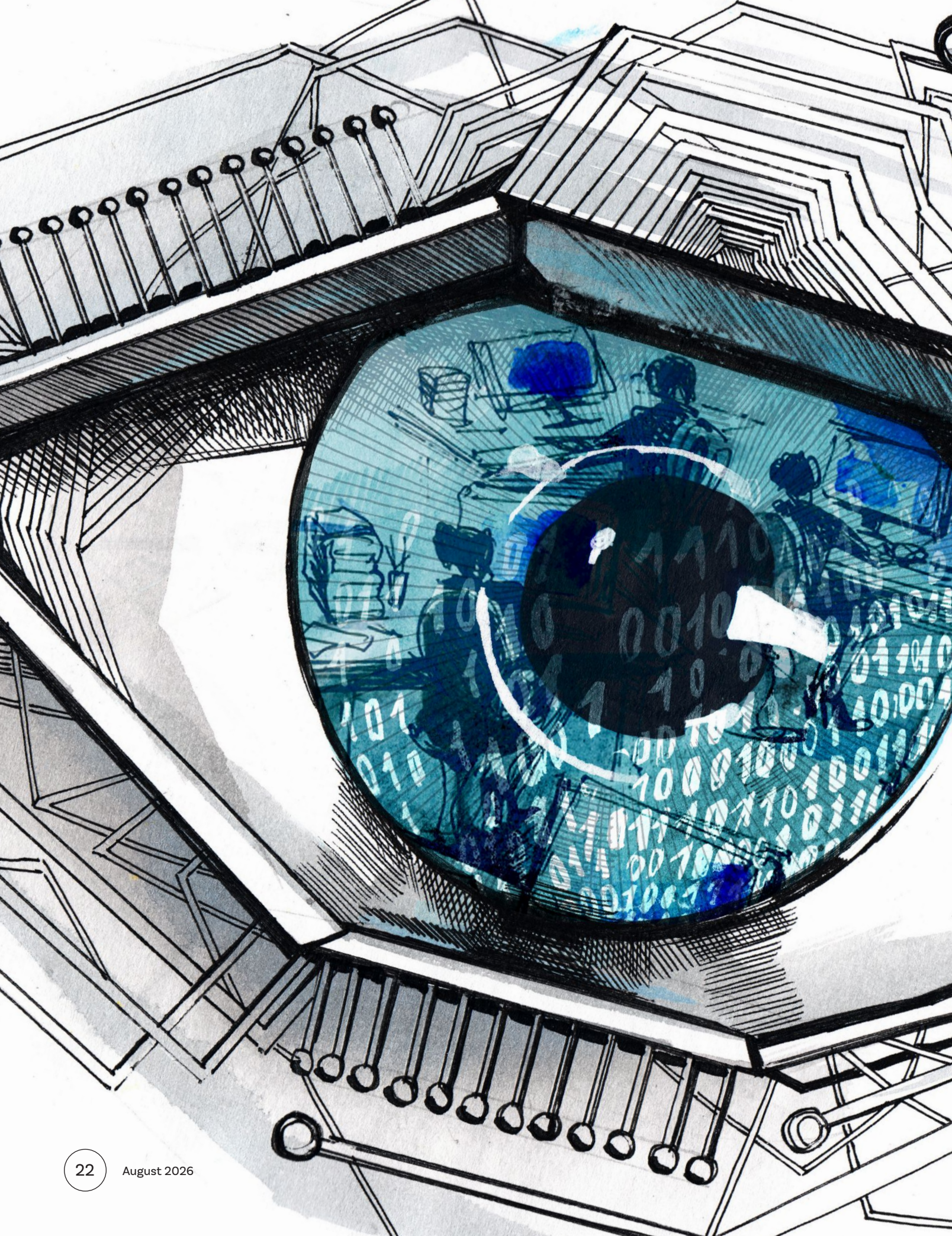
Sham employment arrangements are a common kickback tactic. When a vendor, referral partner, or affiliated entity places an individual on its payroll, internal auditors should scrutinize whether that person performs bona fide work. Compensation tied to referral volume — rather than time, skill, or deliverables — may signal a kickback disguised as wages. Auditors should verify that such employees have documented duties, active supervision, and compensation structures unrelated to referral activity.

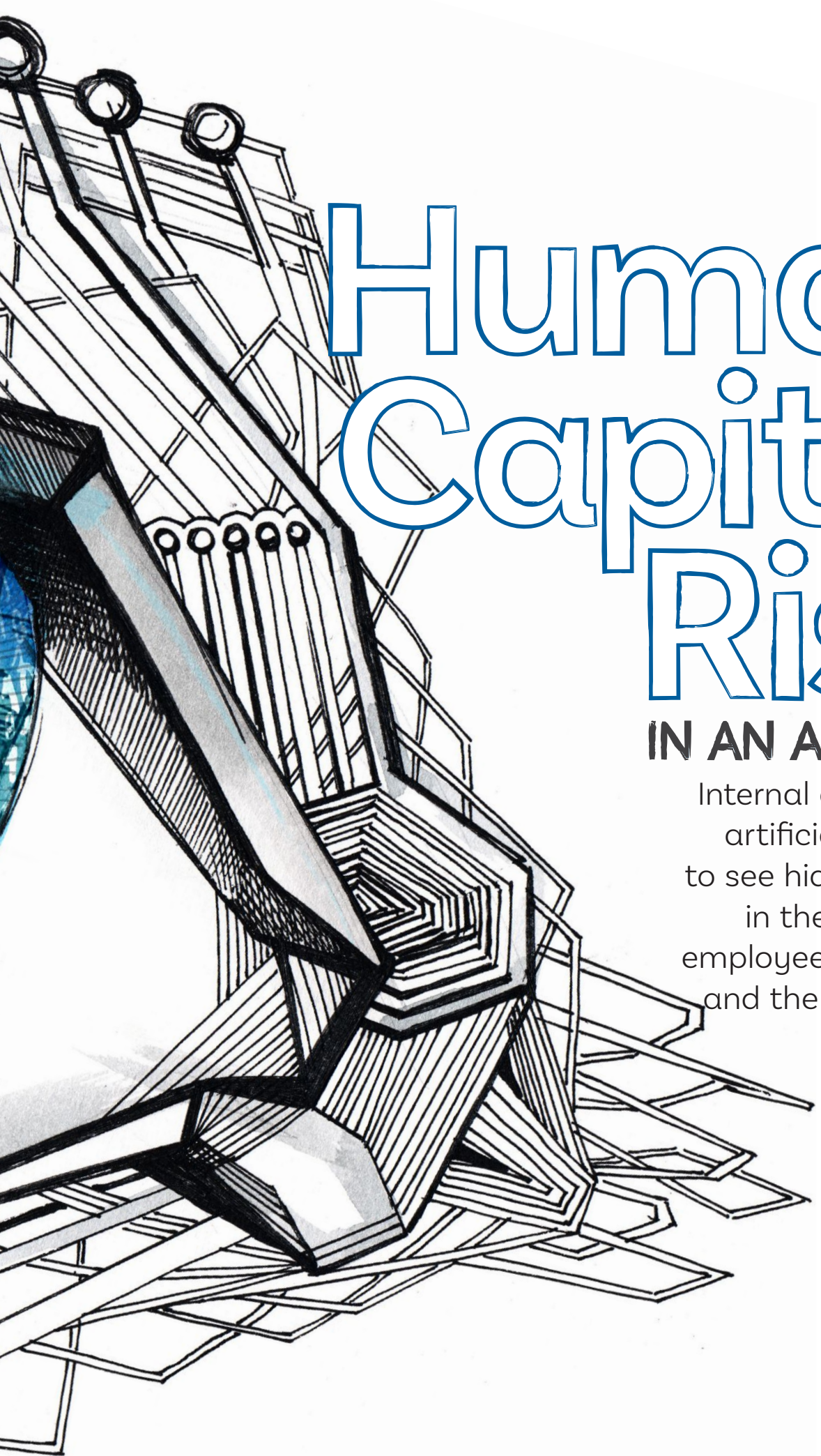
Shell entities and layered payment flows are red flags. Internal auditors should flag vendor and contractor payments that flow through intermediary entities with no clear business purpose. This risk is higher when those companies are created at the same time as the referral relationship.

Contractual exclusions of illegal activity do not equal compliance. The original Pinnacle-Meridian Rx agreement explicitly excluded federally reimbursed prescriptions, which are covered by the Anti-Kickback Statute. Far from being a safeguard, this clause is evidence of intent: The executives knew the law and structured around it. Internal auditors should treat explicit carve-outs in referral agreements as a red flag worth investigating.

Whistleblower lawsuits can reveal fraud. Under the False Claims Act, private citizens — including former business partners, vendors, and employees — can file *qui tam* lawsuits on behalf of the federal government and collect a portion of any funds recovered. For healthcare organizations, robust compliance and internal whistleblower programs with genuine anti-retaliation protections and accessible reporting channels may help uncover concerns internally, reducing reputational damage.

Consistent oversight is needed to prevent multi-entity schemes. Pinnacle ran kickback arrangements with two pharmacies, using different payment structures for each. Companies that provide management or administrative services to multiple healthcare organizations must apply consistent Anti-Kickback Statute compliance controls across all relationships. Oversight should extend beyond the largest or most visible arrangements, and internal auditors should map all referral relationships and payment flows across the full provider network.





Human Capital Risk

IN AN AI WORLD

Internal audit can use artificial intelligence to see hidden patterns in the behaviors of employees, customers, and the organization.

Thomas Diamante, Richard Chan, and Manuel London

Olha Kalinichenko

Employees are an organization's greatest asset, but when mismanaged, they can also be a source of risk. Human capital risk encompasses a wide swath of issues, such as employee misconduct, unfair employment practices, leadership that acts in unnecessarily authoritarian or inappropriate ways, or corporate dynamics that undermine governance, sustainability, and controls.

Artificial intelligence (AI) offers internal auditors new ways to zero in on human capital risk. There are many possibilities to deploy AI as an early warning system, depending on the business or organizational priorities. AI can monitor and flag risks related to customer relationship management, fraud, physical safety, bullying, cultural issues, and organizational dynamics that threaten performance.

AI can also identify organizational ineffectiveness that is a consequence of what leaders fail to do, such as neglecting to escalate risk, provide feedback to underperforming employees, or identify gaps in talent management.

Used within emails or chats to analyze sentiment, or alongside data analytics, AI can find patterns of risk. However, there is a caveat: Overuse of AI monitoring can veer into what feels like a surveillance culture, resulting in diminished morale, stress, and attrition. Further, organizations must exercise the utmost care where AI is used in decision-making, as algorithmic discrimination could result in unfair employment practices.

With the right controls, the organization can balance the use of AI without making employees fearful or paranoid. Internal audit can advise senior management on AI's impact on people, processes, and outcomes to help reduce risk and build competitive advantage.

Individual Risks

The use of AI cybersecurity tools for risk management is now a booming industry, with software to monitor emails, chat interactions, keystrokes, and performance analytics. These tools can be used to analyze content in messaging platforms to get ahead of bullying and incivility issues, thereby preventing sexual harassment lawsuits and protecting morale. One example of this is the AI-based SafeChat+ feature used by DoorDash to safeguard drivers. The app monitors customer messages to identify potentially violent or conflict-prone interactions, enabling drivers to cancel orders without penalty.

A more long-term method involves analyzing anonymous email content by department and over time to uncover problems. For instance, an analysis of words used in email and text exchanges that suggests conflict and disagreement could reveal a particularly authoritative or punitive leadership style.

In looking at procurement, AI can unmask unusual buying patterns and messages that signal inappropriate arrangements like off-ledger payments with suppliers. AI tools can also be used to uncover conflicts between purchasing decisions and vendors, such as contracts that reward self-interest.

AI can even be used to identify AI misuse by employees. The rate of misuse is troubling, with 44% of employees admitting to inappropriate use of AI, which could expose trade secrets or sensitive financial information, according to KPMG's Trust, Attitudes and Use of Artificial Intelligence: A Global Study 2025.

Systemic Risks

Looking for risk within organizational practices or everyday operations is another application for AI. The technology can be used to root out stalled initiatives that absorb funds, dissect high volumes of customer or user complaints to pinpoint root causes, and identify excessive time spent in meetings.

On the human resources (HR) front, AI can identify actions that affect hiring and promotion rates for protected classes, such as women and minorities. Seemingly neutral policies can produce disparate outcomes for these groups because of biases that hiring managers do not recognize or would not admit. Auditors can track these patterns by region or department to strengthen talent acquisition, promotion, and retention practices, while reducing legal risk.

AI can also see trends in employee complaints against management, including illegal actions such as sexual harassment and financial misconduct. Used by internal auditors, AI can complement whistleblowing programs by surfacing issues that employees may be reluctant to raise through traditional channels.

As a culture risk diagnostic, AI gives organizations an ear to the ground, providing a powerful means to strengthen risk culture. That said, because AI lacks intentionality and moral judgment, leaders must be cautious: Leaning too heavily on algorithmic findings can undermine the relationships and trust a healthy culture requires.

Organizational Dynamics

AI can also alert internal auditors to patterns of behavior or decision-making

that point to risk. Behavioral patterns are easier to detect in the aggregate, making them well suited to AI.

Specifically, internal auditors can use AI systems to reveal problematic signs of behavior among leaders, especially for teams under stress. For instance, AI can analyze group discussions and leader communication patterns to identify actions that impede rational decision-making. One indication of this is groupthink, where team members agree with each other without discussing alternative points of view. A more subtle demonstration of ineffective group behavior when stress is high is a tendency to make riskier decisions, as groups under stress tend toward less cautious decisions than individuals would reach on their own.

Other, more nuanced applications would be the identification of decisions by senior leaders that are misaligned with organizational values or ignore socially responsible criteria that are important to the board and stakeholders. Such decision-making patterns can inform the HR, risk, and governance professionals guiding the organization.

AI can help internal auditors uncover high-stakes human capital issues — intentional or unintentional disruptions, subversive actions, and passive aggression. By scrutinizing AI-assisted decision-making, auditors can see who gets heard, how conflicting priorities interact, where incentives distort oversight, and how frontline pressure shapes behavior. This enables internal audit to detect organizational dynamics that signal failure, including:

- ***Behavioral drift*** — gaps in actions, decisions, and follow-through.
- ***Control failures*** — unintentional or deliberate breakdowns of procedure.
- ***Systemic cracks*** — misaligned incentives, weak performance management, and ineffective leadership.

AI can also reveal emerging vulnerabilities: information hoarding, workarounds, inconsistent customer treatment, bypassed controls,

AI can analyze discussions and leader communication patterns to identify actions that impede rational decision-making.

unexplained role changes, disempowered teams, unsustainable workloads, and eroding customer trust. These are all indicators of misbehavior that can threaten organizational performance.

Monitoring Is Not Management

AI-driven management systems, cloaked as data-based management or evidence-driven behavior and performance tools, can easily create a surveillance culture. With such early-warning systems, employees may learn to distrust management, growing fearful of being watched, measured, and criticized for every stroke of the keyboard (see "A Slippery Slope Into Surveillance Culture" on this page). Yet, enabling technology to touch employees in such a way that it captures productive and counterproductive behavior is fast becoming commonplace.

In a 2025 Pew Research Center survey of more than 5,000 employees, U.S. Workers Are More Worried Than Hopeful About Future AI Use in the Workplace, 52% of participants report being worried about the future use of AI at their company. Only a small fraction say they expect it to improve their own opportunities. Roughly one-third anticipate fewer long-term job prospects because of AI.

A 2023 Pew survey, AI in Hiring and Evaluating Workers: What Americans Think, suggested that realizing efficiencies at the expense of employee trust and morale would be counterproductive, with workers showing skepticism about the use of AI for workplace monitoring and evaluation. Indeed, 61% of survey respondents say they oppose more invasive AI applications such as physical movement tracking and digital activities, 81% say AI monitoring would lead to workers feeling "inappropriately watched," and 66% worry the data would be misused.

Organizations must balance between preventing bad risks through controls and monitoring with nurturing the collaboration and innovation that enable good risks. A healthy risk culture in the AI world guards against harmful risk and supports good risk-taking. Wrongdoing averted; innovation sparked.

To support innovation while avoiding unnecessary risk, internal auditors should:

Think like an integrator. Diffused responsibility for AI often leads to a lack of accountability. As an integrator, internal audit can help the organization align AI use across the organization through controls. In addition, assuming accountability for monitoring the impact of AI on people, processes, and outcomes would enable the profession to advise the C-suite on how best to use the technology to accelerate execution and build competitive advantage.

Inspect AI output to guard against blind acceptance. Internal audit can ensure that useful metrics are in place to assess AI's value. By focusing on business and employee outcomes and asking the right questions, internal audit can assure management that controls are in place to reduce unwanted human capital risk.

A SLIPPERY SLOPE INTO SURVEILLANCE CULTURE

AI-based monitoring can catch employees unawares. Consider this scenario.

Before his annual performance review with the department manager, Joe Karlsson, a senior analyst, gathers notes to be fully prepared for what he expects will be a robust, appreciative, and helpful conversation. The analyst makes a mental note to ask questions like, "What can I be doing better?" or "Tell me how I can add additional value?" Coming off a solid year of performance, Karlsson is feeling confident as the review begins.

"As you know, we are moving toward a more data-based, or evidence-based, performance management philosophy," the manager, Anna DeHart, reminds the senior analyst at the start of the conversation.

"Sounds good," Karlsson replies. "I led several initiatives and achieved more than a few milestones this year."

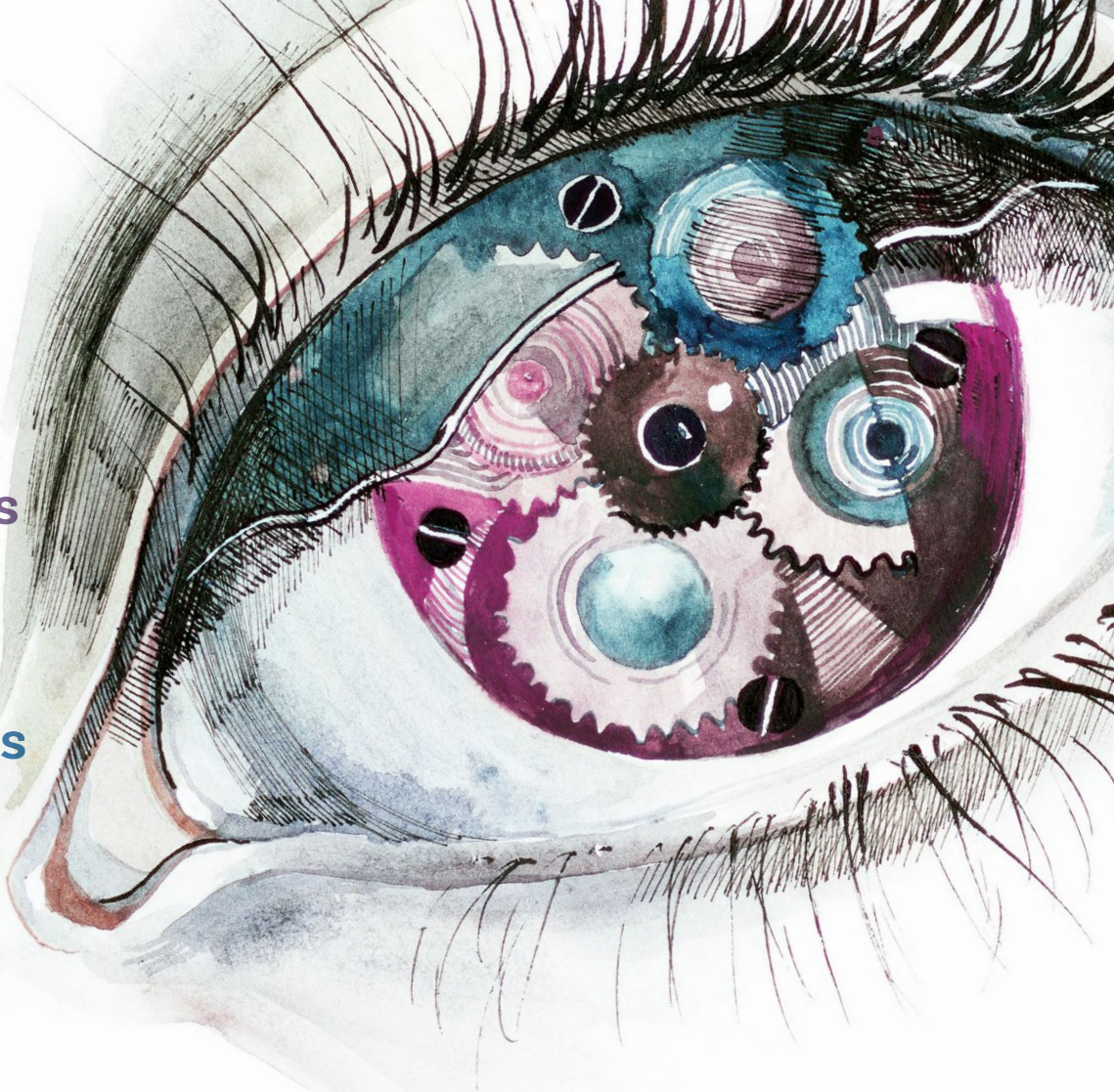
"That's great," the manager says. "Can you tell me why you only attended 65% of the process review meetings? I thought this was a crucial operational efficiency initiative?"

Karlsson is taken aback. "That can't be right!"

"It is," DeHart says. She explains that the company uses software to track behavioral risk, and one metric is attendance at all operational meetings.

"While we are still in the virtual realm, it is noted that you are on camera only 33% of the time, and the data also shows that your keystrokes are in the 80th percentile compared to others during these virtual operational meetings," DeHart says. "This level of inattentiveness to such important projects is worrisome."

A healthy risk culture in the AI world guards against harmful risk and supports good risk-taking.



Internal audit should help create guardrails to reduce AI-related human capital risk. However, leadership must own the risk. Internal audit can assure executives that they are engaged in the right activities to thwart unwanted, unhealthy, AI-related human capital risk by offering a structured checklist of tasks and safeguards:

- Inventory all AI tools that have been used for monitoring and managing human capital.
- Assess whether AI tools have a documented business purpose, legal basis, and business rationale.
- Test data flows by examining data sources, storage, usage, retention periods, and disclosure.
- Advise on employee transparency practices.
- Flag the trust and morale risk explicitly in reporting.
- Challenge management to demonstrate that metrics derived from AI monitoring predict performance.
- Question any personnel decision where AI output was created without a human review.
- Verify human-in-the-loop controls operate as designed for high-stakes decisions, such as hiring, firing, and promoting employees.
- Ensure employee challenges to AI decisions are tracked, resolved, and fed back into model governance.

Toward a Healthy Risk Culture

Internal auditors should use culture stress testing not only to fortify internal controls, but to assess how people respond to organizational change. Transitions such as software implementations, increased monitoring, mergers, acquisitions, and initial public offerings generate emotional and behavioral reactions that manifest as measurable risks — employee turnover risk, diminished productivity, distrust, fear, miscommunication, and battles over conflicting priorities.

These are not soft issues; they are early warning signs of a control breakdown. AI can help surface and monitor these human factors in ways traditional risk frameworks often miss.

Thomas Diamante, PHD, is president and organizational psychologist for Diamante Metrics LLC in Stony Brook, N.Y.

Richard Chan, PHD, is a professor of management at Stony Brook University in Stony Brook, N.Y.

Risk Focused. Future Ready.

The IIA's 2026-2027 Global Board chair, **Stacey Schabel**, says internal auditors must help organizations navigate an interconnected and technology-driven risk environment.

Historically, internal audit has delivered tremendous value by helping organizations understand what happened, why it happened, and whether controls operated effectively. That foundation remains critical, but in today's environment, assurance alone is no longer enough.

Organizations are operating in a world where risks are increasingly interconnected, technology-driven, and moving at an unprecedented pace. Cybersecurity threats, artificial intelligence (AI), geopolitical uncertainty, regulatory change, workforce transformation, and shifting stakeholder expectations are converging in ways that create new challenges for boards and executives.

As risk continues to evolve, so must internal auditing. The organizations internal auditors serve need more than hindsight. They need assurance, insight, and foresight. They need professionals who can help them understand emerging risks, identify how risks interact and compound one another, and provide perspective that supports better decision-making.

Previous IIA Global Board chairs all helped advance the internal audit profession in ways we needed to move forward. I intend to continue this evolution in a way that positions the profession for the future. That is why my theme as the 2026-2027 Global Board chair is "Risk Focused. Future Ready."

Being *risk-focused* means aligning internal audit's efforts to the risks that matter most to organizational success. It means looking beyond traditional audit plans and ensuring we are providing insight and foresight around the strategic, operational, technological, and emerging risks that can have the greatest impact

on our organizations. Internal auditors must help boards and executive teams protect against those risks that can cause real harm to their company's reputation, sustainability, and ability to meet strategic objectives.

Being *future-ready* means preparing internal auditors and their organizations for what comes next. It means embracing innovation, strengthening digital and AI fluency, advancing new ways of working, and equipping the next generation of professionals with the skills needed to thrive in a rapidly changing environment.

By becoming risk-focused and future-ready, internal auditors can strengthen our value, increase our impact, and elevate our role as strategic advisors to our organizations and their stakeholders.

From Assurance to Foresight

Boards and executives are looking for more than assurance nowadays. They are looking for strategic perspective. They want help understanding what is waiting for them around the corner, where risks are emerging, how these risks may affect their goals and priorities, and how to mitigate them.

Today's strongest organizations align risk management, assurance, governance, and strategy in a coordinated and forward-looking way. Internal audit is uniquely positioned to make this happen and to provide this foresight by seeing across functions, connecting patterns, identifying emerging issues, and helping prioritize activities that support long-term success.

When internal auditors talk with executives and board members today, the conversation is different from conversations we've had in the past. Increasingly, the focus centers around uncertainty. It's not that risk is new; organizations have always faced risk. What's different now is how cyber threats, regulatory pressure, stakeholder expectations, and other risks are all rapidly scaling and amplifying one another.

These risks can feel a lot like everything, everywhere, all at once. A cyber event can quickly become a regulatory issue. A lack of skilled talent can inhibit innovation and operational performance. A supply-chain disruption can simultaneously damage customer trust, financial performance, and strategic success.

Amid these risks, business leaders must make decisions faster than ever. They need help managing increasingly complex environments and mitigating the risks they face. Internal audit can help them navigate this environment and add stability.

One way internal audit can do this is by coordinating with first-line leaders and second-line teams, such as risk management and compliance. We can create an integrated assurance view across top risks, highlighting the state of key controls and mitigating activities, and the related internal and external assurance and assessment work. Such an integrated assurance plan can provide clarity around how well the risks that matter most are being managed. It also can identify gaps, help prioritize activities, and inform decision-making.

Our profession's future is not defined by what we audit. It is defined by how effectively we help organizations navigate an increasingly linked and technology-driven risk environment.

A Global Impact

One of the most rewarding aspects of my involvement with The IIA has been seeing firsthand the profession's ability to create meaningful change on a global scale.

Earlier in my career, I became involved with what was then known as the Global Financial Services Guidance Committee, working with fellow volunteers to develop practical guidance for the financial sector. During that time, I worked with a seasoned colleague to navigate a regulatory and risk-related challenge. That experience showed me how The IIA's guidance helps organizations address complex, emerging risks and gives boards, regulators, and practitioners clear and consistent direction.

My work on that committee, and others, reinforced something I continue to see in action today: When the profession comes together to solve important challenges, our impact extends far beyond an individual organization. That's the thing I love about The IIA — the impact we're making around the world. Through our Global Internal Audit Standards, guidance, advocacy, thought leadership, and global community, we are helping strengthen governance, improve organizational resilience, and build trust around the world. That's really powerful.

Priorities for the Profession

The IIA's Vision 2035 goals are worth working to achieve. As Global Board chair, I want to help ensure The IIA is well positioned to achieve that vision by focusing on areas where we can make the greatest difference. To that end, I have identified five priorities that support Vision 2035 and will help strengthen both our profession and The IIA for the future.

First, I want to position internal audit as a strategic, risk-focused advisor. Internal audit has the greatest impact when it aligns its work to the risks that matter most. By

helping organizations identify emerging risks, strengthen resilience, and make better decisions, we can play a critical role in protecting and creating organizational value.

Second, I want to lead the profession through AI, cyber, and digital change. AI is transforming organizations at an unprecedented pace and amplifying other top organizational risks. While this technology creates tremendous opportunities, it also introduces new governance, cybersecurity, ethics, privacy, and workforce readiness risks.

One example is Anthropic's Claude Mythos model, which can assess an organization's environment and define an attack path that exploits unpatched vulnerabilities in a matter of minutes. The introduction of this frontier AI tool — and others like it — amplifies every organization's cyber and third-party risks and requires urgent, fundamental changes in how these risks are managed and mitigated. Internal auditors must develop the knowledge, skills, and digital fluency necessary to help organizations mitigate these and other AI-related risks swiftly and effectively, and to govern AI responsibly.

Third, I intend to champion integrated assurance, enterprise risk management (ERM), and the Three Lines Model globally. As risks become more tightly

The Changing Velocity of Risk

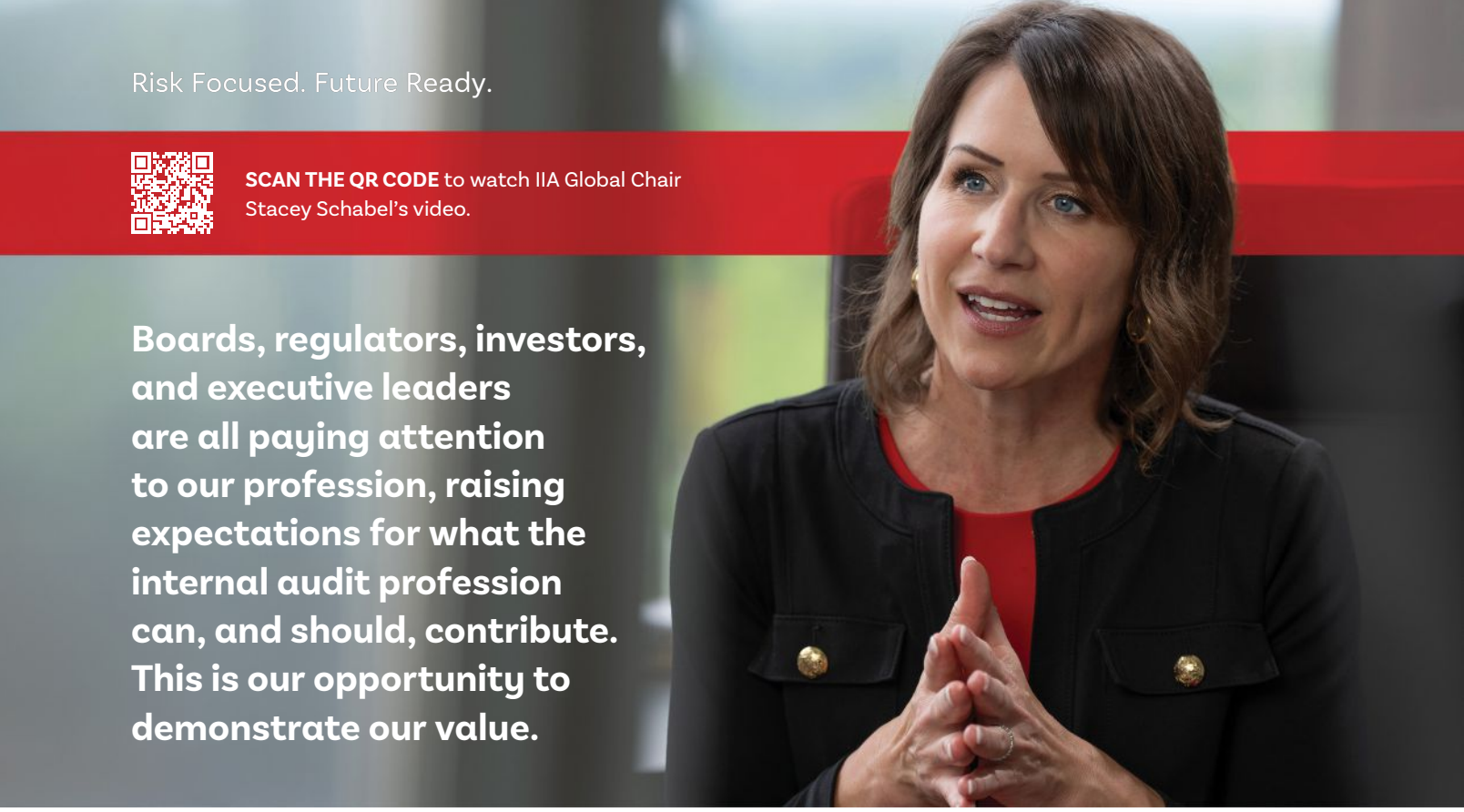
Today's organizations manage whole ecosystems of risks simultaneously, with various risks influencing one another in ways that never happened in the past. In fact, the difference between the past and present is exponential in this regard.

Before, top risks included topics such as compliance, financial controls, and operations, which were more linear and isolated. They were still significant risks, but they were less dynamic and interconnected than the risks internal auditors need to think about today.

Now, cybersecurity, AI, geopolitical, and other risks are accelerating and amplifying one another. A geopolitical problem in one region can affect operations or disrupt supply chains globally. A single operational disruption can create financial, compliance, and strategic consequences, all at the same time.

This changing velocity and volume of risk means organizations need stronger alignment, clearer visibility, and better coordination across functions.

SCAN THE QR CODE to watch IIA Global Chair Stacey Schabel's video.



Boards, regulators, investors, and executive leaders are all paying attention to our profession, raising expectations for what the internal audit profession can, and should, contribute. This is our opportunity to demonstrate our value.

connected, organizations need greater coordination among risk management, compliance, and internal audit functions and business leaders. The Three Lines Model remains a powerful framework for helping organizations provide clarity around roles and align governance, risk, and assurance activities to achieve their objectives (see "The Changing Velocity of Risk" on page 31).

In July, The IIA issued a Statement of Position that updates the Three Lines Model to emphasize the value of collaboration, coordination, and reliance among the three lines and external assurance providers. Such integration reduces duplication, improves visibility, strengthens accountability, and supports integrated assurance, providing leaders with a more complete view of the risks they face. Similarly, The IIA has published The Role of Internal Auditing in Enterprise Risk Management, a Statement of Position that depicts the value of coordination across ERM activities and where internal audit contributes.

Fourth, I plan to strengthen advocacy along with board, audit committee, and governance effectiveness. Strong governance has never been more important. Through advocacy, thought leadership, and engagement with policymakers, regulators, boards, and audit committees around the world, The IIA has been elevating — and must continue to elevate — internal audit's contributions to organizational success, trust, and resilience.

Fifth, I intend to invest in the next generation of the profession. Preparing a future-ready profession requires attracting, developing, and empowering tomorrow's internal auditors. By investing in education and professional development, we can build a pipeline of future-ready talent.

Being Intentional

When I reflect on the future of our profession, I see tremendous opportunity. Organizations are navigating increasingly complex environments and questioning what this means for their risks, technology, governance, and resilience. Internal auditors can help answer those questions.

Boards, regulators, investors, and executive leaders are all paying attention to our profession, raising expectations for what the internal audit profession can, and should, contribute. This is our opportunity to demonstrate our value.

By remaining risk-focused and future-ready, internal auditors can help organizations navigate uncertainty, strengthen trust, and achieve their objectives. At the same time, we can ensure The IIA and the profession continue to evolve and add value for generations to come.

Stacey Schabel, CIA, CPA, is senior vice president and global head of operational risk at RGA, based in St. Louis.

Boards Need to Up Their Game

Internal audit can help boards bolster governance amid change and growing risks.

Anita Dennis Joshua Clark

97% of companies are undergoing a significant transformation or are about to start one.

SOURCE: EY-PARTHENON CEO OUTLOOK SURVEY, JANUARY 2026

It is an extraordinary time to be a corporate director amid rapid change and disruption. Executive search and consulting firm Spencer Stuart says, "Board members are under pressure like never before."

Expectations for boards and their organizations are increasing. "We're in a new age of proactive value identification, orchestration, and realization," says Sarah Francis, EY global client service partner and Center for Board Matters managing director, in Richmond, Va. "The board has a tremendous role to play." Francis was one of the speakers at a January event in Washington D.C., to launch The IIA Global Audit Committee Center (see

"Audit Committee Center" on this page.)

Many boards may not be prepared for the challenges they face. The refreshment rate of board members is slowing, the board talent pipeline is narrowing, and there is a gap between the artificial intelligence (AI) knowledge that directors have and what boards actually need, according to the Global Board Institute's The Global State of Boards & Governance 2026 Report.

Internal auditors are well-positioned to provide the information and advice that can enhance board effectiveness. The IIA's Internal Audit: Vision 2035 report says internal audit's future lies in taking a more forward-looking role as strategic advisors. That includes a key role in advising the board on strategy, says Hiroshi Naka, director, Audit Committee, on The IIA Global Board of Directors and a former vice president and auditor general of the World Bank Group.

Map the Journey

As an objective advisor, internal audit can help boards gain a clear-eyed view of their own strengths and weaknesses. "A robust and well-designed board evaluation process is a critical component of corporate governance," Francis says. Many stock exchanges require or encourage publicly listed companies to conduct annual board evaluations and charter reviews. However, organizations in dynamic sectors, such as technology, might want to conduct them semi-annually to address issues that arise between check-ins, according to Ann Cohen, IIA executive vice president and chief financial officer, who is also an independent board member of Niagen Bioscience Inc.

Internal audit can determine whether the board's governance policies are being followed and what impact they have, says Sally Clark, audit committee chair at Citigroup Global Capital Markets Ltd. and a nonexecutive director at Allied Irish Bank. In addition, she recommends internal audit leverage the Global Internal Audit Standards to drive change and provide independent, data-driven risk assessments that can highlight areas in need of attention. Internal audit can also use The IIA's Risk in Focus 2026 results to open up meaningful conversations on current and emerging threats, she notes.

An evaluation is an opportunity to step back and take stock. "There must be a proper annual appraisal of the board to ask: Are the individual members coming to the party?" says Tshepo Mofokeng, CAE at the Sefako Makgatho Health Sciences University in Pretoria, South Africa and director, Global Research, on The IIA Global Board. "Are the committees doing their work? Is the full board achieving its mandate, based on the board charter?" This assessment should look not only internally but also at the company and its goals. "It is also an opportunity to ensure the board's work aligns with the strategy of the organization and its compliance considerations," he says, "and to determine whether the board and committees' charters are in sync."

AUDIT COMMITTEE CENTER

The IIA Global Audit Committee Center provides thought leadership, strategic insights, and resources to help boards and audit committees strengthen internal audit oversight and drive governance excellence. Its offerings include newsletter alerts, governance insights, research reports, webinars, in-person events, and access to thought leadership that is aligned with The IIA's Vision 2035 initiative and the Standards. It is designed to elevate internal audit's profile and impact in the boardroom by helping audit committee members better understand their oversight responsibilities and internal audit's strategic value. The IIA has also established a Global Audit Committee Center Board of Directors, representing six regions — North America, Latin America, Europe, Africa, the Middle East, and Asia-Pacific — to guide the Center's global strategy and ensure its initiatives reflect regional perspectives.

"There must be a proper annual appraisal of the board to ask… Is the full board achieving its mandate?"

Tshepo Mofokeng, CAE, Sefako Makgatho Health Sciences University // Director, Global Services, The IIA Global Board

To encourage independent reviews, internal audit can recommend that external facilitators or evaluators, such as executive search and professional services firms, conduct objective evaluations. Director interviews and anonymous peer reviews can be used to evaluate the level of participation and expertise. The results can drive necessary member rotations, director education plans, and board refreshment. "Take that feedback and translate it into composition and capability changes on the board," Cohen advises.

Board charter reviews should ensure charters reflect current regulatory requirements and evolving risk, Cohen says. Major events should also trigger charter revisions, including mergers and acquisitions, cyber incidents, restatements, or new regulations. For example, in South Africa, a new iteration of the country's corporate governance reporting rules, King V, forced many boards to reexamine their charters, Mofokeng says.

Stay Up to Speed

During disruptive times, boards should return to the basics of risk management, Naka says. Boards should analyze various categories of risk — financial, technological, operational, and reputational — and consider the threats surrounding each one, he says.

Internal audit's expansive view of the organization can be invaluable in this effort. The internal auditor's "day job is really to get a bit of a helicopter view of an organization," Clark says. "You might spot three things going wrong in different parts of the organization and be able to identify common linkages or themes." A board's responsibilities are much the same.

Internal audit can also help boards revisit key risks overshadowed by other problems. For example, "requirements to disclose sustainability information matter a lot in terms of the financial statement," Naka says. While AI is a hot topic now, organizations should not neglect other evolving risks.

Staying current on threats and opportunities requires rethinking some practices. "Boards need to move away from the standard check-the-box approach to a more forward-looking governance model," Cohen explains. That will require developing disciplined agendas focused on high-value issues, she says.

The right mix of capabilities is also vital for effective governance. Board members should possess business acumen and core competencies in areas such as accounting, legal, human resources, and information and communications technology, but boards must also continuously develop new skills in areas like new technologies and cybersecurity, Mofokeng says.

Cohen recommends that boards receive regular briefings from external specialists on relevant political and economic trends, as well as from advisory boards in specialized areas. With significant topics like AI, boards can assign oversight to a dedicated technology committee or set up a specific subcommittee of the audit committee to prevent oversight gaps, Clark says. These groups can ensure the board considers AI's opportunities and risks. "It's really healthy for boards to think about themselves as learning organizations, just as organizations do," she explains.

One of Clark's boards calls its training "provocation sessions." They focus on important issues not typically found on board agendas, such as learning about behavioral sciences to better understand culture. The goal,

> "Boards need to move away from the standard check-the-box approach to a more forward-looking governance model."
>
> **Ann Cohen**, Executive Vice President and CFO, The IIA // Board Member, Niagen Bioscience Inc.

> "Requirements to disclose sustainability information matter a lot in terms of the financial statement."
>
> **Hiroshi Naka**, Former Vice President and Auditor General, World Bank Group // Director, Audit Committee, The IIA Global Board

Clark says, is to move from a passive awareness of trends to an active understanding of their implications.

Recruit the Right People

According to the Global Board Institute's report, the highest-performing boards see composition as a strategic asset to be optimized, "not a roster to be maintained." Francis says she sees a rising demand for nimble thinkers and people with operational crisis management experience.

"They have the agile mindset, as well as the mobilization experience around big transformations," she says. "They've taken calculated risks. They have that crisis management muscle that instills confidence with investors and with management."

Clark chaired the independent review committee of the Chartered Institute of Internal Auditors that created a new Internal Audit Code of Practice for the U.K. and Ireland. She cautions against choosing new directors who fit the traditional stereotype of retired leaders with strong financial or operational skills, while bypassing candidates whose skills are focused on technology or other emerging capabilities.

Seventy-six percent of directors expect AI to be a factor in their company's growth strategy, but 66% say they have limited or no AI knowledge, according to the Global Board Institute. The right candidate who is more knowledgeable about AI "may be younger, and therefore you can't expect someone to have all the same characteristics that they might have done in the days of old," Clark says.

Looking beyond board composition to the entire organization and its culture, Clark notes that The IIA's Organizational Behavior Topical Requirement gives internal auditors new guidance on assessing how well an organization's culture aligns with its ethics and values. As a result, "boards have a massive opportunity to harness internal audit functions to do more," she says.

Build for the Future

Board refreshment can help ensure a diversity of experience. Francis encourages boards to address tenure, retirement age, and replacing directors whose skills no longer fit the board's needs.

Last year, the 418 directors who left S&P 500 boards had an average age of just under 69 and an average tenure of just under 12 years, according to the 2025 U.S. Spencer Stuart Board Index. Mandatory retirement age was cited as the main reason for board turnover, and 64% of boards set it at 75 or older, compared to only 34% that had the same requirement in 2015. The report concluded that boards need to consider relevance, contributions, and

succession issues "and act on what they learn."

Boards should modernize their skills matrix annually to incorporate soft skills such as curiosity, adaptability, and the ability to challenge management constructively, Cohen says. To identify the best candidates, she recommends boards conduct structured interviews and case discussions, as well as reference checks focused on how candidates collaborate and how well they operate in ambiguity.

Boards need strong leaders and equally strong successors. Cohen recommends developing a multi-year succession plan that ensures a smooth transition. That means developing a slate of potential board members and setting retirement guidelines to bring in new talent and prevent leadership gaps. Internal audit can help boards assess the skills and viewpoints they need to face ongoing challenges.

Maintaining Effective Governance

Given the high expectations for boards, internal auditors can help maintain effective governance through their knowledge of how boards operate and how their decisions unfold over time. In putting their expertise to work in an advisory role, Mofokeng recommends that internal audit:

- Assist the board in creating its strategy matrix.
- Advise on a digital transformation strategy based on internal audit's own use of new technologies.
- Offer insights on risk management and whether it is being handled efficiently and cost-effectively.

Internal auditors can also provide strategic advice to help boards address new and emerging risks. To take on this role, internal auditors must shift their emphasis from compliance, Naka explains. "They will have to change their focus to strategy review," he says.

As part of the board's early alert system, internal audit can provide predictive analysis and other data-based insights for strategic evaluation and assessment, Francis says. Clear presentations that connect findings to strategy help boards get full value from internal audit's insights.

Ultimately, internal audit should build a deeper relationship with the board, Clark says. "I would encourage heads of internal audit to reach out to board members to begin a two-way relationship," she says.

When she was chief internal auditor at Barclays, Clark met regularly with the chairs of the audit and risk committees to discuss risk management from an audit perspective, as well as with the board chairman quarterly. "Now that I'm a board member, I really enjoy those interactions," Clark says. "Internal audit leaders should assume that board members would be quite happy to have these discussions."

> "[Disruption] requires board members who are dynamic and who have experience leading through unpredictability."
>
> **Sarah Francis,** Global Service Partner and Managing Director, Center for Board Matters, EY

> "I would encourage heads of internal audit to reach out to board members to begin a two-way relationship."
>
> **Sally Clark,** Audit Committee Chair, Citigroup Global Capital Markets // Nonexecutive Director, Allied Irish Bank

Leading Through Unpredictability

Boards must accept new approaches. "When the risk universe has changed, it does not mean the solution that we're going to propose would be palatable to the board all the time," Mofokeng says.

As organizations and business models face disruption, "it requires board members who are dynamic and who have experience leading through unpredictability," Francis says. Internal audit can provide the assurance and insights boards need to succeed.

Anita Dennis is a freelance business writer based in Maplewood, N.J.

The NextGen Audit Mentor

A customized AI agent helps an internal audit function onboard new practitioners by delivering personalized guidance and career support.

Sarah Kuhn Rheya Tanner Cole

Integrating artificial intelligence (AI) into internal audit workflows has transformative potential. That's why, with the buzz around agentic AI growing louder by the day, I couldn't resist the urge to build something, myself. But first, I needed a use case — something practical and easy to implement.

Unlike traditional models that simply respond to questions, agentic AI interprets user objectives, breaks complex tasks into manageable steps, and adapts dynamically as new information becomes available (see "What Is Agentic AI?" on page 40). In internal audit, this means an AI agent can do more than answer questions — it can guide auditors through processes, suggest resources, and check for conformance with the Global Internal Audit Standards. In short, it can act like a human mentor.

For auditors, this capability opens the door to consistent, on-demand mentorship — especially valuable when human coaches are unavailable. As a mentor, agentic AI could help my internal audit function solve one of its biggest challenges: onboarding. I envisioned a digital audit mentor that could guide new staff members through our methodology, answer questions in real time, and provide immediate feedback.

The goal was simple: ensure every new auditor

What Is Agentic AI?

Agentic AI marks a significant evolution in AI. It moves beyond reactive, prompt-based systems toward autonomous, goal-oriented collaborators.

The arrival of generative AI (GenAI) like ChatGPT and AI image generators showed that machines could do more than retrieve or classify information — they could create, producing coherent text, code, artwork, and other media from minimal prompts. This leap in creativity and contextual understanding laid the groundwork for deeper, more autonomous forms of intelligence.

Through iterative improvements, GenAI enabled models to grasp nuance, context, and intent with increasing sophistication. Prompt engineering has become an art, but users still need to guide the system step-by-step.

The limits of these tools revealed a new frontier: What if the AI could take the initiative, orchestrate multistep processes, and adapt its strategies based on shifting objectives? Agentic AI answers that question by building on the generative base, adding layers of agency, autonomy, and decision-making.

What makes agentic AI powerful is its ability to learn from each interaction. It refines its approach over time, offering increasingly personalized support.

received consistent foundational knowledge and ongoing support, regardless of when they joined or which team they were assigned to. By delegating routine guidance to an AI agent, experienced auditors could then focus on strategic challenges, while new team members receive tailored support. The result? Improved audit quality and efficiency across the board.

The Onboarding Challenge

In our company, internal audit relies heavily on a rotational staffing model, welcoming auditors from a variety of backgrounds into the department for fixed periods. This system injects fresh perspectives and adaptability into our work, but it also means that many new recruits don't receive sustained mentorship or the benefit of shadowing seasoned professionals over long stretches. They are immediately met with the steep learning curve of internal audit standards, organizational protocols, and the demands of our audit methodology.

Simultaneously, internal audit's most experienced auditors — those best suited to serve as mentors — are often deeply engaged in high-stakes audits or strategic projects and aren't available for hands-on coaching or to answer every question that arises. As a result, onboarding can lack the structure and reinforcement needed to ensure new auditors are confident, competent, and aligned with our department's standards. Agentic AI was an opportunity to change that.

Building the Audit Mentor

Our company had been using Microsoft Copilot for about a year, so I was familiar with its strengths — summarizing, editing, and locating information. But I also knew its limitations. It sometimes pulled outdated or inaccurate data.

Recently, internal audit was given the ability to build its own custom agents. This gave us a chance to "ring-fence" the information the tool could access. By limiting the agent to approved methodology, training materials, and professional guidance, we could reduce the risk of outdated or irrelevant responses and keep its answers aligned with how the audit function works.

Surprisingly, building the agent was straightforward. I started by experimenting with pre-built agents to understand their structure and the level of detail required. Then I had the option to build one from scratch or describe the agent's configuration via chat.

Three core components were needed: description, instructions, and knowledge.

Description. For Audit Mentor, as we call it, I used the following description:

"An agent to help train new internal auditors, act as a mentor for new and experienced auditors, train auditors leading an audit for the first time, and give career advice."

Instructions. These were more detailed directives:

- Answer questions based on reference material (files or web links).
- Offer frequently asked question (FAQ) lists based on reference material.
- Break down jargon into everyday language.
- Give examples.
- Offer learning plans.
- Ask for feedback.
- Help with refining the prompt.
- Conduct mock conversations or offer practice examples/scenarios auditors might encounter.
- Use internal audit's methodology to answer questions first, then reference the Standards or IIA Global Practice Guides.
- Reference sources such as the COSO frameworks and other related governance, risk, and control frameworks.
- Use The IIA's Internal Auditing Competency Framework to show the skills and expectations of auditors; emphasize discussing learning plans with supervisors.

Knowledge Base. I uploaded a mix of internet links and internal training files. Internal audit's methodology and charter provide the foundation for all the agent's responses. The Standards, Practice Guides, and eventually the Topical Requirements are secondary sources for the agent to reference.

Next, I added written examples of each of the COSO *Internal Control–Integrated Framework* principles, based on a training document designed for new auditors. I also added a template with generic examples of each COSO principle to help auditors scope engagements during audit planning.

Another important resource was a white paper on governance, risk, and control, which establishes how all the COSO principles work together to help internal audit assess the control environment, control design, and control effectiveness. Rounding out the agent's knowledge base were supplemental materials such as the Internal Auditing Competency Framework, internal audit's quality assurance review template, and the Three Lines Model.

Ready for Launch

Built using Microsoft Copilot, Audit Mentor is a customized AI agent supporting auditors at every stage of their careers. The agent blends adaptive technology with audit expertise to deliver personalized guidance, simulate real-world scenarios, and reinforce internal audit's methodology — while maintaining enterprise-grade security.

To test Audit Mentor's capabilities and limitations, I asked a wide range of common and nuanced audit questions. I rated each response to pinpoint recurring issues and fine-tune both the agent's instructions and its knowledge base.

For example, our methodology was missing the standard report distribution list, despite it being a frequently sought-after document. Updating the methodology and including the distribution matrix as a key source document ensured future users would have easy access to this information.

The next phase involved sharing the agent with a small, trusted group of experienced auditors who could provide thoughtful, candid feedback. This pilot group's insights were invaluable in identifying strengths and areas for improvement. This phase revealed an unexpected technical constraint: Only users with full Copilot licenses could access the agent. This limitation underscored the importance of infrastructure in rolling out new tools. Fortunately, the company later purchased enterprise licenses, paving the way for future expansion.

Feedback from pilot users was overwhelmingly positive. While some wanted more detailed responses, the agent consistently delivered accurate, relevant guidance — and improved with continued use. After a month of iterative testing and updates, we opened access to all licensed users in the department. While adoption was gradual, once auditors experienced its practical value, the tool became a vital resource within the team.

Agent in Action

Audit Mentor tailors onboarding paths based on role, experience, and audit domain. For new auditors, the agent builds learning plans focused on methodology, standards, and mock audits. It explains frameworks like COSO and the Three Lines Model in everyday language and helps develop audit scope and test plans.

One standout feature is Audit Mentor's ability to simulate "what if" scenarios. Auditors can pose hypothetical challenges, such as evaluating documentation or planning a risk-based audit, and receive detailed, context-aware responses. As one pilot user noted, the agent "adjusted well and gave much more useful insights" when questions included more context.

Audit Mentor

The AI-powered assistant supports internal auditors at every stage of their work, from onboarding to leading engagements. Audit Mentor provides methodology-aligned answers tailored to the auditor's experience level.

Training New Auditors

How do I get started? Can you build a learning plan based on methodology and IIA Standards?

Mentoring Experienced Auditors

What are some best practices for conducting an audit?

Mock Conversations

Can you provide a practice scenario for an audit?

Leading an Audit

What should I focus on when leading an audit for the first time?

General Methodology

I have a question about methodology. Can you tell me about [ ] and why it is important?

Feedback

Give me feedback on [ ]. Have I met the objectives based on methodology or the Standards? [paste text]

In practice, Audit Mentor can assist with developing audit scope and test plans, ensuring that all relevant areas are covered. It can also help auditors evaluate documentation against the Standards, providing a second layer of review that enhances the quality and accuracy of audit findings.

The agent references uploaded materials to ensure alignment with professional standards. It helps set expectations of competency, align workpapers with methodology and IIA guidance, and helps auditors prepare for internal quality reviews. It also explains how it sources its answers, promoting transparency and trust.

The agent is personal and can comment on individual progress, highlight strengths, and identify areas for improvement. It generates custom reports on learning outcomes, which auditors can use to set goals and address training gaps. Feedback loops — like thumbs up or thumbs down ratings — help refine responses over time.

The company's auditors have used Audit Mentor to:

- Build learning plans and mock audits.
- Evaluate documentation against standards.
- Develop audit scope and test plans.
- Ask questions about methodology in an FAQ-like fashion.

Moving Into the Future

From initial build to departmentwide adoption, the process revealed both the promise and the challenges of introducing new tools into established practices. One obstacle was trust. Some auditors had already experienced inaccurate or unsupported responses from general AI tools, so they were skeptical that a customized agent could stay within defined boundaries and provide relevant, fact-based guidance. Others had not used Copilot at all, which meant the challenge was less about overcoming skepticism and more about helping them see how the tool could be useful in their daily work.

Ultimately, adoption depended on two things: encouraging auditors to use the agent consistently and helping auditors trust the quality of its responses. Over time, as users saw that Audit Mentor could provide grounded, practical guidance, confidence and usage grew.

The positives greatly outweighed the difficulties. Audit Mentor has streamlined access to knowledge, improved consistency, and fostered community ownership. Looking ahead, Audit Mentor sets a strong precedent for future AI initiatives.

Sarah Kuhn, CIA, CRMA, CCSA, is principal audit consultant for an energy company and is based in Bartlesville, Okla.

Internal audit can help research and development functions manage risk, enable innovation, and strengthen governance.

Flavia Rusu Nitu, Laetitia Robillard, and Teri Petree

TRANSFORMING PHARMACEUTICAL R&D

The pharmaceutical industry is undergoing major transformations to improve efficiency, reduce costs, and accelerate access to life-saving treatments. Innovations such as machine learning, telemedicine, remote monitoring, and artificial intelligence (AI)-enabled drug discovery are reshaping research and development (R&D) and accelerating access to critical treatments and personalized therapies.

This transformation is accompanied by heightened governance expectations. Audit committees and senior executives are seeking greater visibility into systemic and emerging risks. This reflects the need for more forward-looking, data-driven oversight in an environment where traditional risk management approaches are no longer sufficient.

In pharmaceutical R&D, internal audit serves as a strategic partner, aligning audit plans with transformation goals to mitigate risks, support innovation, ensure regulatory compliance, and prioritize patient safety. Through continuous assurance and evaluation of transformational initiatives, internal audit strengthens organizational resilience. Moreover, internal audit's data-driven methods and strategic insights foster transparency and help R&D functions at the world's largest pharmaceutical companies navigate this complex and changing environment.

Internal Audit's Evolving Role

Internal audit is shifting from a traditional assurance function to a strategic partner in organizational change and a real-time risk radar to help businesses balance risk and opportunity. Technologies such as AI, machine learning, and digital platforms drive R&D innovation but also introduce risks such as hallucinations, algorithmic bias, data breaches, and data governance gaps. This is particularly relevant as organizations invest in these technologies to drive R&D innovation.

At the largest pharmaceutical companies, internal audit has embraced this change by expanding the audit universe and using new approaches to control testing. Traditionally, internal audit coverage of R&D included laboratory and human subject research, intellectual property, data governance, human biological samples, third parties, and other areas of risk inherent in a pharmaceutical company. The audit universe comprised non-repeated, customized audits.

Today, leading companies use data analytics and AI to determine what to audit, and within each audit to evaluate and test samples. Audits now assess whether AI investments deliver measurable improvements in efficiency, risk detection, and decision-making, and whether these outcomes are sustainable and aligned with strategic objectives.

Partners in Innovation

As a strategic partner, internal audit provides advisory and assurance services to guide organizations through significant change. One way auditors contribute is by conducting joint risk reviews during proposed organizational, system, or process transformations. Rather than only reviewing the outcomes of these initiatives, practitioners participate in the design phase by highlighting risks, informing decisions on operating model design, and assessing cultural readiness.

Organizations often request these joint risk reviews and advisory services, which are conducted in partnership between internal audit and the R&D business, to leverage internal audit's expertise. Drawing on experience across business units, auditors can identify risks, share best practices, and highlight key opportunities to drive change.

To support large-scale change programs, audit functions use structured methodologies, including:

- Process maps to identify critical areas tied to objectives, compliance, and quality. This tool enables auditors to evaluate existing controls, identify gaps, and develop a risk control matrix that balances innovation with control effectiveness.
- Actionable risk and activity frameworks to move from the current state to the target state.
- Light-touch advisory audits that provide recommendations without issuing formal findings, maintaining an efficient and collaborative approach.

Internal audit contributes in different ways at key stages

of transformation projects. During the design phase, internal audit serves as a sounding board for process and system designers to ensure risk management is integrated and aligned with strategic objectives.

In the implementation phase, internal audit provides proactive feedback on risk management and recommends ways to address blind spots during rollout. After the transformation is completed, internal audit can review new processes and systems, assess progress against goals, and advise on the transition to normal operations.

Internal audit's strategic value lies in balancing both risk mitigation and efficiency. This balance helps transformation efforts meet compliance and performance goals while supporting sustainable success.

Course Corrections

Beyond evaluating progress, internal audit should recommend course corrections to refine transformation strategies and maximize benefits. This approach helps pharmaceutical organizations stay flexible, adapt to unforeseen challenges, and stay focused on overarching goals.

Lessons from past transformation initiatives can inform current and future programs. Through assurance engagements, internal audit can capture lessons learned and preserve institutional knowledge, helping the organization avoid recurring mistakes and apply successful strategies. This knowledge helps the organization manage change more effectively over the long term and strengthens its ability to innovate.

From Data to Insight

In today's regulatory environment, ensuring data integrity across R&D, especially in clinical trials, is crucial for pharmaceutical sponsors. This requires rigorous oversight, transparency, and controls to maintain compliance and reliability. Thirty-five percent of audit committees seek better insights into systemic governance risks, while CAEs prioritize advanced risk assessment and technology-driven solutions, according to Gartner's Leadership Vision for 2025: Chief Audit Executive report.

Novartis' internal audit function addressed these needs by developing an innovative clinical risk detection and monitoring tool using AI, machine learning, and data analytics. This tool aggregates clinical trial data, flags trends based on key risk indicators, and delivers actionable insights.

Using a customer-centric approach, internal audit worked with R&D stakeholders to identify key challenges and future needs for the tool to address. Cross-functional partnerships with quality assurance, enterprise risk, compliance, data governance, and data privacy functions helped ensure the solution addressed AI-related privacy, compliance, data integrity, and audit requirements.

The custom tool helps internal auditors identify new risk areas in governance, oversight, and risk management that otherwise might go uncovered. By adding granular, data-based insights at the site and field levels to broader qualitative assessments, the tool helps auditors expand risk coverage, detect enterprise risks earlier, and tailor oversight. This approach has reinforced reliability across the R&D ecosystem and improved risk management.

The Novartis case study underscores the importance of risk mitigation frameworks, integrated assurance, and data-driven insights focused on enterprise-level risks. Predictive risk intelligence and advanced assessment tools create new opportunities for internal audit, including:

- *Improved risk detection.* Early trend identification enables internal audit to anticipate risks and recommend enterprisewide corrective actions.
- *Enhanced collaboration.* Greater data access fosters cross-functional teamwork and a unified response.

DRAWING ON EXPERIENCE ACROSS BUSINESS UNITS, AUDITORS CAN IDENTIFY RISKS, SHARE BEST PRACTICES, AND HIGHLIGHT KEY OPPORTUNITIES TO DRIVE CHANGE.

- *Increased efficiency.* Advanced tools reduce manual efforts, allowing auditors to prioritize strategic advisory roles.

Audit Planning Reimagined

In recent years, internal audit functions at GSK and Sanofi have been reimagining the audit planning process, itself. Moving beyond traditional approaches, internal audit works with R&D leaders to develop an audit plan that examines innovation and risk, from decision-making frameworks to digital transformation opportunities.

This approach focuses on value creation from the first interaction. During pre-scoping discussions, auditors engage stakeholders to understand their needs and ensure each engagement aligns with R&D's strategic objectives.

Transformation-focused engagements now represent a significant portion of Sanofi's and GSK's R&D audit plans. The scope of these audits now covers governance assessment and emerging risks such as AI and data analytics, process optimization, and third-party oversight. Each audit links findings to strategic objectives or the control framework, fostering a culture of continuous improvement.

Three key success factors underpin this approach:

- A team of strategically minded auditors who combine scientific understanding with the ability to be a catalyst for change.
- Cross-functional expertise spanning R&D, general business, change management, and digital technologies.

- Integrated data science and AI capabilities.

GSK and Sanofi's improved risk management and the R&D organization's willingness to self-evaluate and prioritize new approaches have enabled this transformation. The outcome for both companies is a more flexible, value-driven internal audit function that supports innovation while ensuring controls remain in place, furthering the strategic partnership between R&D and internal audit.

Built for Change

The examples from leading pharmaceutical companies underscore the importance of collaboration, innovation, and agility, and other pharmaceutical companies are pursuing similar efforts. Supported by advanced data analysis, internal audit is positioning itself as a key partner in R&D transformation while maintaining compliance.

Internal audit has moved beyond its traditional gatekeeping role in the pharmaceutical industry. Amid R&D transformation, its adaptability, innovation, and integration ensure processes remain compliant, efficient, and forward-looking. By leveraging AI-enabled tools, auditors are uncovering systemic risks and strengthening patient safety — key pillars of a thriving pharmaceutical ecosystem.

Internal audit's success lies in its agility and strategic involvement, enabling pharmaceutical companies to navigate uncertainty, address emerging risks, and achieve ambitious R&D transformation goals. By focusing on customer needs and using advanced data analytics, internal audit is helping R&D functions drive results, maintain compliance, and protect shareholder value in a challenging, dynamic environment.

Flavia Rusu Nitu, CIA, is audit director, R&D and Strategy and Growth at Novartis and is based in Basel, Switzerland.

Laetitia Robillard, PHD, is head of Internal Audit, R&D/Medical at Sanofi and is based in Paris.

Teri Petree, CIA, is a senior director and audit account director, R&D at GSK and is based in Raleigh, N.C.

Fabien Saint-Gerard, CIA, internal audit functional head director, R&D and Strategy & Growth at Novartis; **Alex Fraga, CISA, CPA,** senior director, corporate audit, R&D and Supply Chain at Pfizer; **Markus Boehringer, PHD,** former internal audit director, R&D and Supply Chain at Roche; **Jillian Fontes, PHD,** internal audit director, R&D, Global Medical, and GPPM at Astra Zeneca; and **Andrew Cooper,** internal audit head, R&D, Global Medical, and GPPM at Astra Zeneca contributed to this article.

INTERNAL AUDIT'S SUCCESS LIES IN ITS AGILITY AND STRATEGIC INVOLVEMENT, ENABLING PHARMACEUTICAL COMPANIES TO NAVIGATE UNCERTAINTY, ADDRESS EMERGING RISKS, AND ACHIEVE AMBITIOUS R&D TRANSFORMATION GOALS.

INDEPENDENT ENOUGH TO MATTER

Internal audit's independence depends on balancing stakeholder engagement with effective guardrails.

Muhammad Shahrukh

Imagine a CAE preparing to enter the boardroom or address senior management about the company's most pressing risks. On paper, internal audit's mandate is clear: independence and objectivity. The Global Internal Audit Standards, the internal audit charter, and the reporting line to the board all reinforce this independence. With that backing, the CAE is confident of being heard and taken seriously.

However, as the meeting unfolds, that confidence is tested. Rather than discussing the top risks, the conversation quickly shifts to financial results, performance metrics, and executive decisions. The room aligns around management's narrative, and the CAE's seat at the table suddenly feels less secure. Stay silent, and the CAE risks irrelevance. Speak up too forcefully, and the CAE may appear to be resistant.

The CAE can raise concerns about culture, controls, or emerging risks, but how will these issues be received? The independence that seemed so clear now feels less certain, caught between credibility and compromise. The idea of independence shifts from a theoretical safeguard to a source of tension.

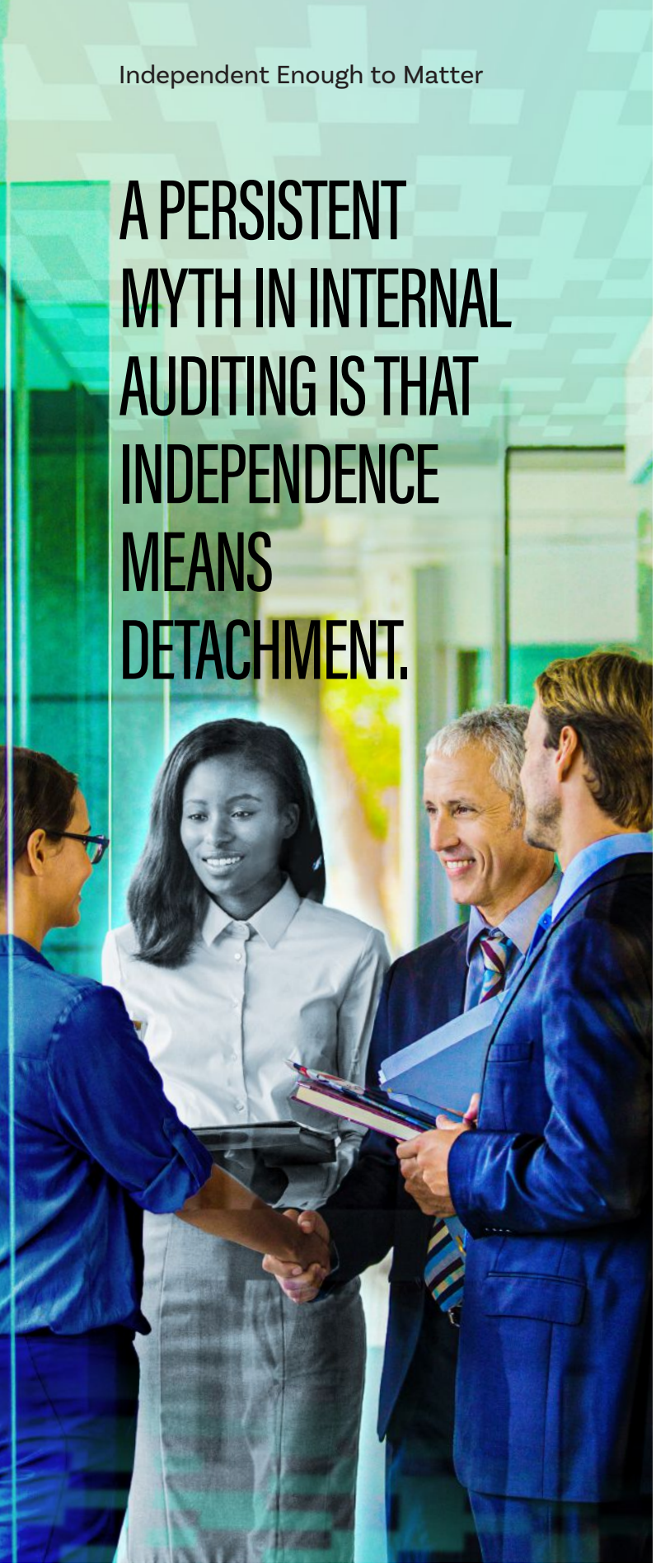
Faced by this dilemma, CAEs may question whether independence is more myth than reality. In practice, complete insulation from management's influence rarely exists. No audit function, no matter how carefully structured, operates entirely outside the organization's environment.

The real issue for internal audit is not whether it can be completely independent, but whether its independence is sufficiently protected and embedded within the organization to give the audit function a voice with the board and management. The question CAEs should be asking is whether internal audit is independent enough to create value for its stakeholders.

WHEN INDEPENDENCE FAILS

A high-profile corporate collapse shows how formal governance structures can fail when internal audit functions can't effectively challenge management. In June 2020, German payment processing company Wirecard filed for insolvency following the arrest of its CEO amid news reports of accounting malpractice. Wirecard's governance structures appeared appropriate on paper — it had both a supervisory board and an audit committee. However, whether because of limited influence, ineffective escalation, or broader governance failures, the company's internal

A PERSISTENT MYTH IN INTERNAL AUDITING IS THAT INDEPENDENCE MEANS DETACHMENT.



audit function was unable to detect one of Europe's largest corporate frauds.

According to reports, internal audit was sidelined at Wirecard, which allowed fraudulent practices to continue largely unchecked. Despite years of allegations, whistleblower concerns, and control deficiencies, internal audit didn't surface or resolve issues before they became catastrophic. Put simply, its independence existed formally but failed in substance.

THE ESSENCE OF INDEPENDENCE

The Standards provide a foundation for defining what independence and objectivity truly mean and require. *Independence* is about organizational positioning and reporting lines that ensure internal audit is free from undue management influence. *Objectivity* is an unbiased mental attitude and a mindset of impartiality.

Independence protects objectivity; objectivity ensures independence has meaning. Whereas objectivity is readily embraced by internal auditors and rarely questioned, the practical meaning of independence is often misunderstood.

Too frequently, independence is treated as a binary: Either you are independent or you are compromised. But reality is more nuanced; independence is contextual, relational, and a principle to be continuously managed.

Internal auditors constantly negotiate their role between management and the audit committee, with independence shaped as much by expectations and relationships as by formal reporting lines (see "Where Independence Is Tested" on page 51). They also are constantly balancing their dual advisory and assurance roles, creating tensions that cannot be reduced to a simple yes or no on independence.

A persistent myth in internal auditing is that independence means detachment. Some auditors hesitate to engage too closely with executives, fearing that offering advice or being present in strategy discussions compromises their standing. Such detachment risks making internal audit irrelevant.

MANAGED PROXIMITY

If independence is neither absolute detachment nor unchecked closeness, then what remains is a practical balance. Independence is not about drawing away from management but about engaging with purpose and discipline. This is where the idea of managed proximity comes in: a model where auditors remain close enough to add value yet independence is safeguarded enough to preserve their credibility.

A useful way to visualize this balance is the passenger-seat metaphor. Internal audit rides alongside management. Auditors can navigate, read the map, check for sharp curves ahead, and remind the driver when fuel is low. However, internal audit never takes the wheel — management drives.

This metaphor captures the essence of independence: Internal auditors can provide assurance and advice yet remain clear that management is solely responsible for executive decision-making. Crossing that line (driving) compromises independence.

The Standards provide practical guidance for navigating this path. They do not assume that independence is protected through detachment. Rather, they recognize engaging with management and the board is part of internal audit's role while emphasizing the need to preserve the function's independence.

According to Domain V: Performing Internal Audit Services, advisory services are permitted, provided internal auditors do not assume management responsibilities. The Standards also recognize that circumstances may impair independence, and they prescribe safeguards to address those situations, such as:

- Annual confirmation of independence to the board.
- Disclosure of actual, potential, or perceived impairments.
- Direct board oversight of the internal audit function.
- The use of independent third-party assurance in areas where the CAE temporarily assumes nonaudit responsibilities.

THE CARE TEST

Internal auditors can preserve their independence by applying the CARE test before accepting advisory roles or becoming involved in management activities:

- ***C**ontrol Test*: Are we advising or controlling the decision?
- ***A**ccountability Test*: Who remains accountable for implementation and the final outcomes?
- ***R**eporting and Safeguards Test*: Has internal audit disclosed potential impairments and put appropriate safeguards in place?
- ***E**xternal Perception Test*: Would the audit committee or a reasonable stakeholder see this engagement as strengthening or weakening independence?

WHERE INDEPENDENCE IS TESTED

Independence challenges vary across organizations, cultures, and regulatory settings. In state-owned organizations, internal auditors may encounter political pressure, making strong disclosure and audit committee support essential. In family-owned businesses, close personal ties and less formal governance dynamics can make it more difficult for internal audit to challenge management objectively and maintain functional independence.

Organizations with limited internal audit resources often require practitioners to undertake a broad range of responsibilities. A small audit function may be asked to participate in projects, support management initiatives, and provide advisory services while still delivering its assurance plan. Without clear boundaries and safeguards, the line between advising and assuming management responsibilities can gradually become blurred.

The CAE plays a critical role in this case to ensure that resource constraints do not compromise internal audit's independence. The CAE may need to decline advisory engagements or project involvement if appropriate safeguards cannot be implemented, even at the risk of management dissatisfaction.

Cultural context can make these challenges even more pronounced. In Western Europe and North America, governance frameworks are well-developed, and boards expect rigorous independence. As a result, internal auditors can rely on formal structures and regulatory support.

In contrast, parts of Africa, the Middle East, and South Asia have more hierarchical cultures and concentrated ownership. This can make it more difficult for internal audit to challenge management, especially if leaders do not actively support independence. In these settings, independence depends less on formal rules and more on the CAE's judgment, credibility, and persistence.

Across all these contexts, the Standards provide a unifying anchor. Independence may be tested differently, depending on cultural and governance norms, but it remains the foundation of trust.

TRUST IS EARNED WHEN AUDITORS ENGAGE, CHALLENGE, AND ADVISE WITH INTEGRITY. INDEPENDENCE IS NOT GAINED THROUGH ISOLATION.

Examples in three governance areas illustrate how these guardrails work in practice.

Cybersecurity. Boards are increasingly anxious about ransomware, breaches, and regulatory scrutiny. Internal audit may review incident response plans, test access controls, highlight risks of outdated patching, and advise on best practices. However, it cannot decide which vendor to hire or which cybersecurity control to implement.

Environmental, Social, and Governance (ESG) Reporting. Sustainability reporting is becoming increasingly important for boards, investors, regulators, and other stakeholders. Internal auditors can advise on control frameworks for sustainability data, benchmark against standards, and raise awareness of reporting risks, but they cannot author the disclosures or own the ESG reporting process.

Data Governance. As organizations adopt artificial intelligence (AI), manage massive volumes of data, and navigate privacy regulations, internal audit can assess data quality controls, identify governance gaps, and suggest improvements. However, the function cannot assume responsibility for making data classification, retention, and compliance decisions.

PRINCIPLES INTO PRACTICE

To maintain its independence, internal audit must take concrete actions to make it a managed, repeatable discipline. Applying practical tools can help the function define and strengthen independence.

Advisory Services Policy and Decision Matrix. Internal audit should establish clear criteria defining the types of advisory services it may provide in its policy, the circumstances under which additional safeguards or audit committee approvals are required, and the activities that are prohibited. The services may be categorized as:

- ***Permitted***: Risk workshops, control design reviews, and governance framework advisory.
- ***Restricted***: Policy development, steering committee participation, project advisory, and vendor evaluation.
- ***Prohibited***: Implementing controls, managing projects, making operational decisions, approving

vendors, and authorizing transactions.

Internal audit can use a simple decision matrix to assess advisory requests against these three categories, ensuring the function remains in an advisory role and does not gradually assume management responsibilities. The internal audit charter should explicitly define the boundaries between assurance, advisory services, and management responsibilities.

Independence Disclosure Template. Internal audit should document actual and potential impairments to independence and communicate them to the audit committee using a standardized format. The template may include the nature of the event or activity, the independence risk identified, and the safeguards applied. It also should detail the responsibilities of internal audit, management, and the audit committee.

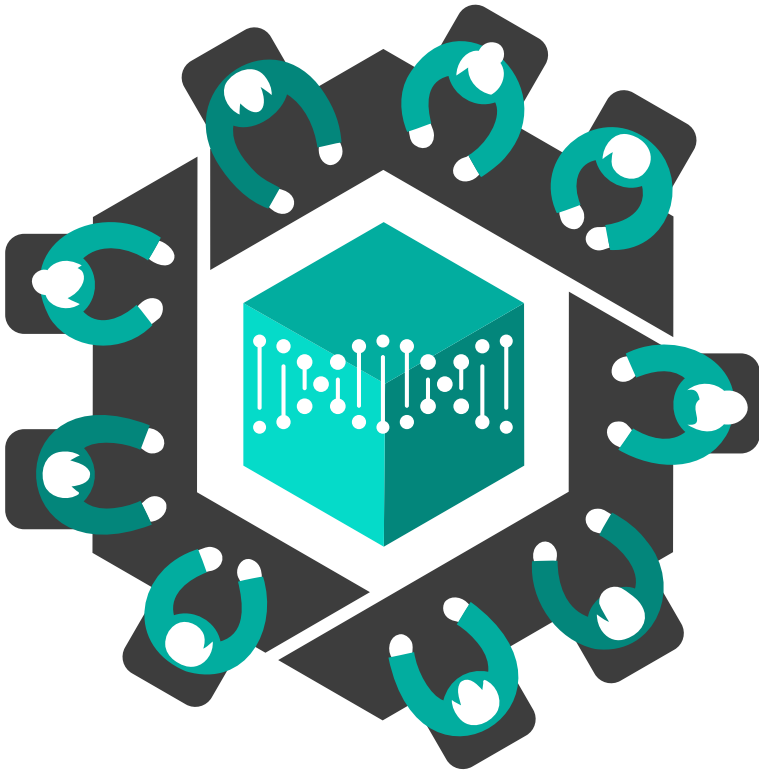
Quality Assurance and Improvement Program (QAIP). Internal audit must periodically assess independence as part of the QAIP. When evaluating conformance with the Standards, internal audit must examine whether advisory activities have affected the credibility of assurance work. They must also determine whether any specific threats to independence have occurred such as management pressure to remove findings and lack of access to required persons or information.

THE BRIDGE

Independence is the currency of trust, the reason boards listen when internal auditors speak. That trust is earned when auditors engage, challenge, and advise with integrity. Independence is not gained through isolation.

Internal audit leaders must move beyond asking, "Are we independent?" Instead, they should start asking, "Are we independent enough to be valuable?" When it is managed well with clear guardrails, independence becomes a bridge between management and the board, between assurance and advice, and between risk and resilience. The greater risk isn't choosing between independence and relevance — it's forgetting that internal audit needs both.

Muhammad Shahrukh, CIA, CA, CPA, is the head of Internal Audit at SAL Saudi Logistics Services in Jeddah, Saudi Arabia.



boardroom

A Better Way of Oversight

COSO's flexible guiding principles aim to help boards improve governance in a complex world.

Matt Kelly

Every organization is unique, so every board must chart its own course for governing it. But keeping a roadmap nearby never hurts.

That's the logic behind COSO's Guiding Principles for Board Oversight, released at the end of March. The guidance is a set of 12 principles that boards can use to ensure that their governance efforts are effective and efficient.

We should also be clear on what the principles are not. They are not a framework akin to COSO's *Internal Control–Integrated Framework* or *Enterprise Risk Management–Integrating With Strategy and Performance*. COSO did release a proposed board oversight framework last year, which weighed in at a hefty 24 principles, plus dozens more points of focus. COSO eventually replaced that proposal in favor of the far more flexible guiding principles.

"It will evoke conversation," says Lisa Halper, a former COSO board member and corporate controller at PepsiCo, who consulted with COSO on the oversight principles. "It's commentary and guidance for boards to enhance their effectiveness over time."

Indeed, COSO emphasized that point in a press release heralding the new guidance. "This guidance is directional and illustrative, not prescriptive," COSO said, "and is intended to complement applicable law, regulation, and governance standards rather than prescribe a single governance model."

"It will evoke conversation. It's commentary and guidance for boards to enhance their effectiveness over time."

Lisa Halper, Former Corporate Controller, PepsiCo; Former Board Member, COSO

OK, message received; boards can use these principles as much — or as little — as they want. But *why* should boards consider following the principles?

That part's easy: With rising risks, demanding stakeholders, and convoluted technology challenges, boards need all the help they can get. "It allows boards to ask themselves, 'Are we still fit for purpose?'" says Karen Narwold, a board director at chemical companies Calumet and Ingevity and mining business Standard Lithium. "Because the world and the board's governance responsibilities are changing."

An Emphasis on Flexibility

The 12 governing principles fall into four broad categories:

- Board foundations.
- Purpose and culture.
- Strategy and enablement.
- Leadership and resilience.

Each principle has a title and one-sentence summary, followed by two paragraphs under a header, "Why this principle matters." The real substance, however, comes in the longer descriptions of how each principle can work in practice in the boardroom, plus a Management Enablement Considerations section that explains how management can help the board put each principle to work.

Take Principle 8, Technology and Data, as an example. First, it states why board oversight of these elements matters: "Technology and data are central to how entities innovate, compete, and deliver value."

The principle then suggests how boards might exercise that oversight, such as asking how management assigns responsibilities among the chief information officer, chief technology officer, chief information security officer, and other leaders. Another example is probing "whether the portfolio of technology initiatives is realistic, given resources and change capacity" and how trade-offs among various IT projects are decided.

Any board could consider those questions, from a publicly traded global company in Europe to a small U.S. nonprofit experimenting with new ways to raise money and offer services.

Don't forget those "management enablement considerations," either. For Principle 8, they include ideas such as the executive team providing technology investment cases tied to the organization's strategic objectives. Another idea is establishing clear lines of accountability for IT management, escalation protocols, and key risk indicators that could go into a board packet.

"For any of us who have worked at a company, yes, the board needs management to help them," Halper says. "Information provided to the board enables directors to perform their fiduciary role."

If the board wants independent assurance that it's following the oversight principles effectively, those management enablement ideas are valuable because they are steps that could be audited. A CAE could use Principle 8's management enablement ideas to build an audit plan for, say, monitoring cybersecurity events or evaluating the return on investment of potential IT projects.

The other 11 principles follow that same approach. The guidance never expressly says a board should do anything. Instead, it favors phrases such as "boards may" (14 times), "boards often" (nine times), and "many boards" (six times), as a subtle guiding hand leading boards toward certain preferred practices.

Principles at Work

A board that wants to implement the COSO board oversight principles could start by considering where its organization sits on the governance maturity curve. Large, established businesses in highly regulated fields may already be following most of the principles, even if directors don't quite know it.

"It allows boards to ask themselves, 'Are we still fit for purpose?' Because the world and the board's governance responsibilities are changing"

Karen Narwold,
Board Director,
Calumet, Ingevity, and
Standard Lithium

"Boards today are tasked with guiding organizations through a far more complex risk environment than they were even five years ago." The COSO principles "provide boards a practical framework for assessing whether their oversight and governance approach remains fit for purpose."

Benito Ybarra, IIA Executive Vice President, Global Standards, Guidance, and Certifications

Those boards could use the principles as fodder for conversation to ask what they might do better.

Small or fast-growing organizations, meanwhile, might use the principles to develop their board oversight practices the right way. "If you're a young company on the immature side of your governance journey, this gives you a structure to help you design the foundations of a good governance program," Narwold says.

Boards could also view the COSO principles through the lens of evolving risks. For example, every board is grappling with the newfangled challenges of artificial intelligence (AI) these days. A board might therefore peruse Principle 1, Board Governance Structure, to consider whether directors need a dedicated IT risk committee, or use Principle 8 to clarify the data governance reports the board wants.

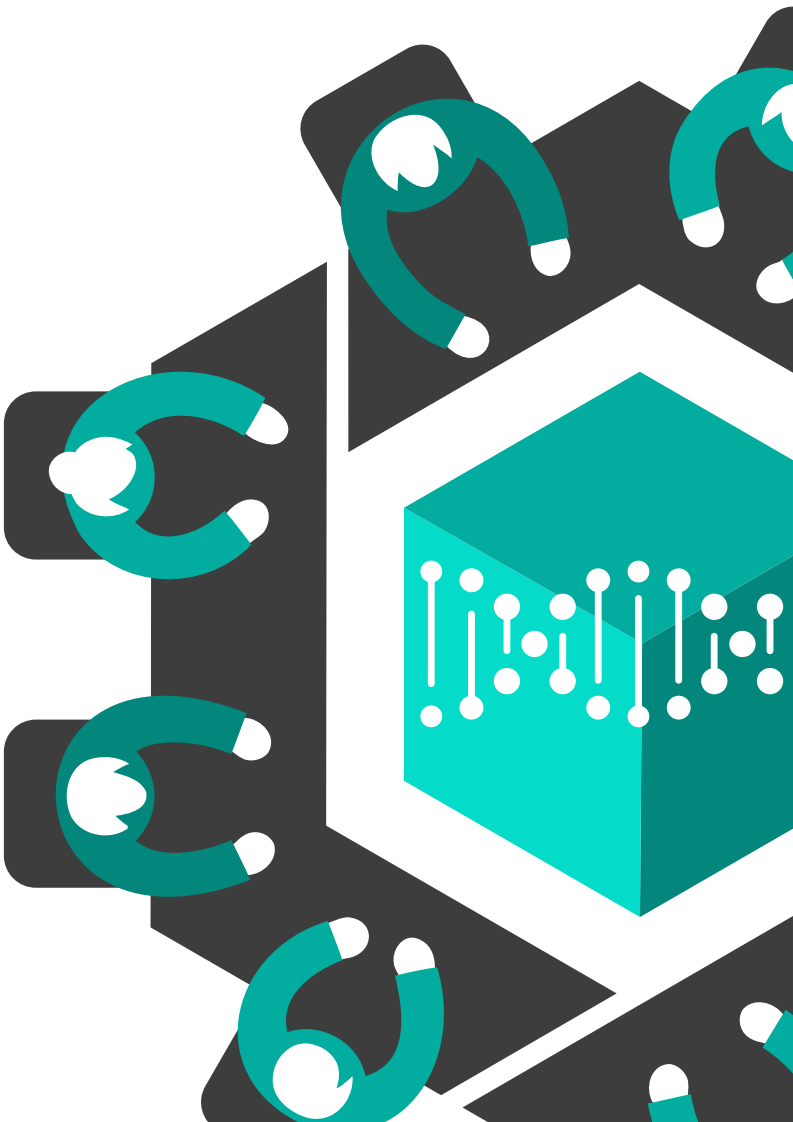
More than anything else, boards need help understanding how they can keep up with the sheer number of issues that are transforming how their organizations fit into the larger world.

"Boards today are tasked with guiding organizations through a far more complex risk environment than they were even five years ago," says Benito Ybarra, IIA executive vice president, Global Standards, Guidance, and Certifications. (The IIA is a sponsor of COSO and helped develop the governance principles.) "COSO developed these principles to provide boards a practical framework for assessing whether their oversight and governance approach remains fit for purpose. The goal is to help boards evaluate not only the risks they face, but whether their organizational structure allows them to operate in a way that supports and enables effective governance."

That could be anything from cybersecurity to AI or from sustainability to business continuity. It's a lot to juggle, and boards need to be deliberate in how they oversee such a vast range of issues. "The board does have its own idea of what governance is, but really it can't stand by itself," Narwold says. "It helps that you can point to something."

The question is whether, in today's endlessly complex operating environment, the board can point to the way forward.

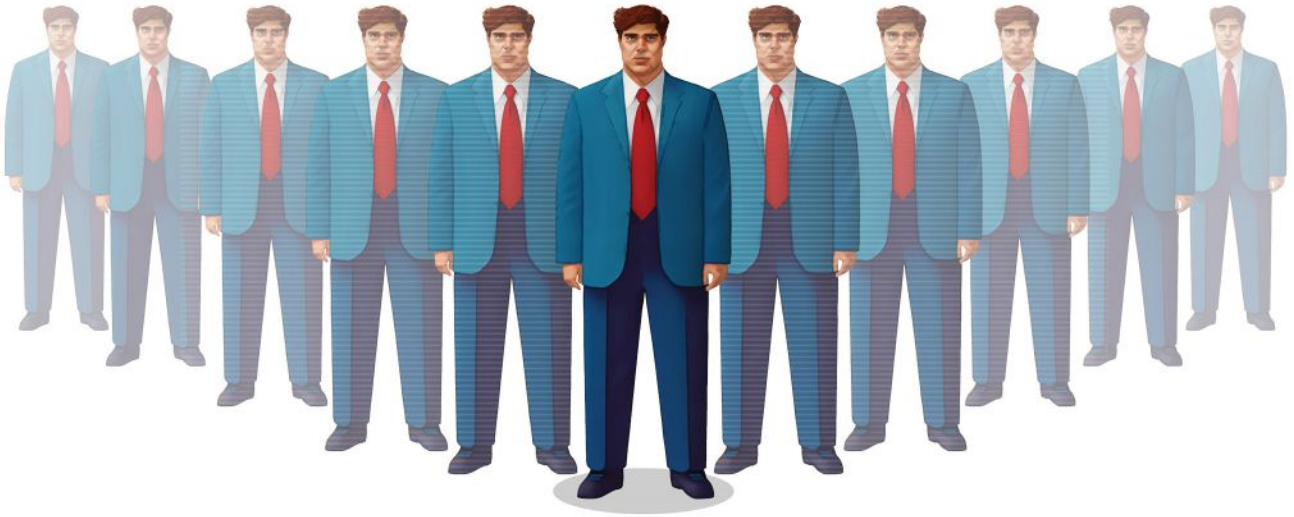
Matt Kelly is editor and CEO of RadicalCompliance.com, an independent blog about audit, compliance, and risk management. He welcomes feedback at mkelly@radicalcompliance.com.



David Salierno

AI is coming for the C-suite: Get ready for the CEO avatar.

Some companies are testing technologies that could transform how leaders communicate, make decisions, and engage employees.



Every executive faces the same constraint: There's only one of them. The CEO's reach may be broad, but a single person can only do so much. Against that backdrop, it's not hard to imagine a chief executive thinking, "What if I could be in multiple places at once?"

Enter the executive avatar — a virtual proxy for company leadership. It's more than a theoretical concept, and some companies are exploring the idea in limited ways.

Sebastian Siemiatkowski, CEO of global fintech Klarna, for example, has used AI-generated versions of himself in earnings presentations. Collaboration technology provider Zoom Communications' CEO, Eric Yuan, has discussed the future possibility of artificial intelligence (AI) "digital twins" of CEOs attending meetings with employees — including executive employees. And according to the *Financial Times*, Meta is exploring an avatar concept for CEO Mark Zuckerberg that could converse with employees and help scale executive presence.

It's a provocative idea and an intriguing vision for the future of leadership. But it also raises fundamental questions about how the technology would be deployed and to what extent the CEO role would remain distinctly human.

"Organizations can't treat executive AI deployment the same way they treat IT automation," says Patrice Williams-Lindo, founder and CEO at Career Nomad, an Atlanta-based workforce intelligence practice. "The risk profile is completely different. When employees can't distinguish between a human decision and a machine simulation of one, you don't just have an engagement problem — you have a governance exposure."

The idea of a digital proxy standing in for the CEO may sound far off, but the underlying technology already exists. And as companies experiment with expanding executive presence through AI, they may face difficult questions around trust, accountability, culture, oversight, and the future role of human leadership, itself.

What Is an Executive Avatar?

For now, the executive avatar is, at best, a loosely defined concept. Depending on the organization's needs and strategy, it could range from a simple communications tool to a digital twin that performs many of the tasks a human CEO would.

More broadly, the AI could help establish, reinforce, and ensure the implementation of the CEO's vision in ways that no single person could accomplish alone. As Williams-Lindo puts it, the avatar could help "anchor the organization to what good looks like."

She adds that organizations may see the avatar less as a standalone IT tool and more as an extension of broader leadership and governance. "The avatar could establish a baseline for the workforce," she says, "one that demonstrates a level of literacy that makes sure governance within the organization is being held to a certain standard."

The potential benefits include helping the executive process large amounts of information more efficiently, identifying trends and blind spots, providing actionable insights, and staying better connected to managers and teams across the organization.

Still, Williams-Lindo says there are clear limits to how far organizations should allow the AI to go. While the technology may eventually support many aspects of executive leadership, the most consequential decisions — particularly those involving crisis response, organizational change, or sensitive interpersonal issues — may continue to require human judgment and emotional intelligence.

"The line is drawn based on the gravity and impact of what needs to be decided,"

Williams-Lindo explains. "Many executive decisions still need to come from a place of human governance."

The Trust Challenge

One of the most difficult challenges of introducing a non-human CEO presence, Williams-Lindo says, will likely be establishing trust. Employees may tolerate and accept the avatar in some contexts, but they could grow distrustful if leadership starts to feel overly automated.

Transparency is essential, Williams-Lindo says. Trust, credibility, and stability comprise what she describes as a "three-legged stool" in organizations. Without those components, even the most well-designed AI may struggle to gain employee buy-in.

That challenge is especially important in situations requiring nuanced communication or emotional sensitivity. Williams-Lindo says organizations would need to define when the avatar steps aside and the human CEO steps in. "What are the flags — the words or language — that require human intervention?" she asks. "There have to be some things that trigger more immediate, human response."

She also says organizations would need to fully disclose the use of avatars and make it clear when employees and stakeholders are interacting with the AI rather than the actual CEO. "There needs to be some sort of disclaimer," she says. "If that type of transparency is missing, organizations risk undermining trust instead of strengthening communication."

Governance and Accountability

Governing an executive avatar may be even more challenging. Unlike many other AI tools, the avatar would operate from a central position within company leadership, wielding strategic influence and executive authority.

That's a great deal of weight for an AI to carry, and Williams-Lindo warns that organizations may underestimate what it takes to deploy these systems effectively and responsibly. "Most organizations are not ready," she says. "They risk trying to scale too fast before properly testing employee readiness and governance processes, rather than taking the time to be truly intentional before they bring in the technology."

While some companies may have pieces of the necessary governance structure in place, relatively few are fully prepared for the pace at which AI capabilities are advancing, Williams-Lindo adds.

Accountability may also be difficult to manage. If an executive avatar spreads misinformation, contributes to a bad decision, or mishandles sensitive company information, tracing responsibility can be tricky. But in Williams-Lindo's view, the buck essentially stops with the human CEO — he or she would ultimately be accountable for the AI's missteps or poor judgment.

"Most organizations are not ready. They risk trying to scale too fast before properly testing employee readiness and governance processes, rather than taking the time to be truly intentional before they bring in the technology."

Patrice Williams-Lindo, Founder and CEO, Career Nomad

The Future of Executive Leadership?

It's far too early to say whether executive avatars may become commonplace. Williams-Lindo says she expects the technology's use to expand, though adoption and the extent of implementation will likely vary depending on culture, risk tolerance, and workforce readiness.

Still, she says, the broader trajectory is becoming clearer, though she does foresee limits to the digital proxy's use. "Do I think it will replace leadership? No," she says. "Do I think it will streamline leadership? Absolutely."

Ultimately, that distinction may define the future of executive avatars. Although the technology might not eliminate the need for human leaders, it could dramatically reshape how leadership is practiced, experienced, and scaled inside organizations. And as companies experiment with AI-mediated executive presence, they may find that the real challenge is not building the technology, itself, but preserving the human trust and accountability that effective leadership has always depended on.

David Salierno is managing partner of Nexus Brand Marketing in Winter Park, Fla.

No Pit Stops

Internal auditors in technology, media, and telecommunications need to get ahead of risk and build teams with technical depth.

Robyn Mishkin, Audit & Assurance Principal, Internal Audit Technology, Media, and Telecommunications Leader, Deloitte & Touche LLP

What risks do technology, media, and telecommunications (TMT) companies face?

The biggest risks in the TMT sector are interconnected, which is what can make them so hard to manage. Cybersecurity is often the most immediate concern, because these companies rely on large digital platforms, cloud environments, connected products, and customer ecosystems that are highly exposed and difficult to fully secure.

At the same time, artificial intelligence (AI) is being embedded into products, operations, content workflows, and customer interactions faster than governance is maturing, which can create new exposures such as intellectual property (IP) leakage like source code exposure, product roadmap leakage, content reuse without protection, model training on protected assets, partner and supplier spillover, and misuse of data. Privacy, third-party dependence, regulatory change, and operational resilience add further pressure.

What makes TMT distinctive is the speed at which one problem can spill into others, turning a cyber event into a privacy issue, a regulatory matter, a vendor problem, and a service disruption all at once. For example, a media company compromise involving unreleased content or proprietary production assets could expose IP, trigger regulatory scrutiny, disrupt distribution channels, and create downstream issues for third-party partners. The sector's significant mergers and acquisitions activity can heighten this risk, as rapid deal cycles can leave newly combined environments with inconsistent controls.

During mergers and acquisitions, where is internal audit the most useful?

Post-merger integration is often where deal value is

either realized or lost, and internal audit has an important role in helping management protect that value. In TMT, integrations are rarely simple. They often involve different technology stacks, data environments, vendor relationships, and operating models — along with cultural differences that are easy to underestimate. Internal audit can help identify where controls are likely to break down, where governance needs to be strengthened, and where compliance obligations may not be fully aligned across the combined business. Equally important, internal audit can warn organizations about operational and cultural friction that slows execution and erodes collaboration. The most effective internal audit functions are involved early, stay focused on the highest risks, and keep asking whether the integration is delivering what the deal promised.

What's at stake with regulatory change?

As requirements such as the European Union AI Act, the General Data Protection Regulation, and U.S. Federal Communications Commission rules continue to evolve, internal audit should focus on whether management can spot new obligations, interpret what they mean, and turn them into workable controls across the business. That often means looking at how teams from legal, privacy, compliance, product, security, and operations work together, including whether the organization has a strong process for keeping pace with evolving requirements.

The risks are not only limited to noncompliance. Unsustainable processes, weak data governance, and delayed remediation can be just as damaging. Internal audit adds the most value when it looks across the whole landscape and helps management connect the dots among cyber, privacy, AI, third-party risk, and resilience.

Parth Jhaveri, Principal, U.S. TMT Leader, Internal Audit & Controls, KPMG US

> What makes TMT distinctive is the speed at which one problem can spill into others, turning a cyber event into a privacy issue, a regulatory matter, a vendor problem, and a service disruption all at once.

How can internal audit at TMT companies get ahead of risks?

Internal audit in the TMT sector is operating in an environment defined by rapid product innovation, evolving business models, and continuously shifting risk profiles. Navigating this pace of change requires a shift from a traditional, retrospective compliance mindset to a more proactive, forward-looking approach.

When companies are constantly changing, a point-in-time audit report based on an annual audit cycle is obsolete the day it's issued. Internal audit teams need to be embedded earlier in transformation initiatives, participate in risk assessment at the planning stage, and continuously refresh audit plans as priorities evolve.

Equally important is adopting more agile ways of working — leveraging continuous monitoring, data-driven insights, and closer collaboration with product and engineering teams. This keeps internal audit aligned as risks evolve in real time, particularly across areas like cybersecurity, data governance, and platform integrity. Ultimately, the function's relevance depends on its ability to act as a strategic risk partner — helping organizations move faster while maintaining strong governance.

How is AI changing internal audit's work and responsibilities?

AI is fundamentally changing internal audit in two ways. As a tool, it helps teams drive efficiency and scale — particularly in planning, risk assessment, and documentation. It enables auditors to focus on higher-value analysis and insight. Many organizations are already seeing tangible benefits in these early-stage use cases, even as broader adoption continues to evolve.

At the same time, AI introduces a new class of risks that internal audit must evaluate independently. These include governance, data quality, bias, third-party dependencies, and explainability. This creates a unique challenge: Internal audit must leverage AI responsibly within its own processes and provide assurance over how the business is deploying it.

What are the talent needs for TMT?

The profile of an internal auditor in TMT is changing. We are moving beyond traditional business process domain knowledge to teams that include real technical depth — data engineers, system architects, and professionals who understand how modern platforms operate.

Today's risks live inside application programming interfaces, cloud configurations, and data pipelines. If a team can't interpret an architecture diagram or understand concepts like shared responsibility in cloud environments, they'll miss real risks.

Just as important is business partnership. Internal audit works with many types of stakeholders, translating complex technical and operational risks into clear, actionable insights that resonate. When audit is seen as a trusted partner rather than a checkpoint, the conversation shifts from "How do we pass the audit?" to "How do we run the business better and safer?"

Teams that combine technical fluency, agility, and strong stakeholder engagement will be the ones that keep pace with the TMT risk landscape.

Internal audit works with many types of stakeholders, translating complex technical and operational risks into clear, actionable insights that resonate.

Certified Internal Auditor®

The Only Globally Recognized Internal Audit Certification

The CIA® is considered a "must have" for internal auditors worldwide. It's the optimal way to validate credibility and ability to effectively and efficiently perform any audit, anywhere, in accordance with the Standards.

Earn it. theiia.org/CIA

CIA®

IPPF

What's New

GLOBAL PRACTICE GUIDE

Auditing Privacy and Data Protection Risks shows how internal auditors can evaluate governance, accountability, and controls across the data life cycle using a flexible approach grounded in global privacy frameworks. **theiia.org/audit-priv-data-protect-risks**

GLOBAL PRACTICE GUIDE

Engagement Planning: Establishing Objectives and Scope details a disciplined approach to engagement planning that helps strengthen governance, risk management, and control while supporting informed decisions and long-term success. **theiia.org/engage-plan-est-obj-scope**

GLOBAL PRACTICE GUIDE

Evaluating the Effectiveness of Ethics Programs helps internal auditors evaluate the scope and effectiveness of ethics programs, define ethical culture in practice, and clarify related roles and responsibilities. **theiia.org/eval-effect-ethics-program**

What's Trending

TOOLS

AI Audit Framework Support Tools help internal auditors and stakeholders assess artificial intelligence (AI) across the organization and strengthen alignment with The IIA's AI Auditing Framework. **theiia.org/ai-audit-framework-sup-tools**

RESOURCE

Artificial Intelligence Knowledge Center. Browse updated events, guides, tools, articles, and podcasts, all curated to enhance internal auditors' understanding and application of AI. **theiia.org/ai**

GLOBAL PRACTICE GUIDE

Internal Auditing Competency Framework provides a practical approach and tools for internal auditors, CAEs, and others to define and meet the expectations of their roles. **theiia.org/comp-framework**

TOPICAL REQUIREMENT

Third-Party. This mandatory guidance provides a comprehensive approach to assessing the design and implementation of third-party governance, risk management, and control processes. It becomes effective Sept. 15, and will now be included in quality assessments and external quality assessments. **theiia.org/tr-third-party**

Coming Soon

TOOLS

AI Prompting for Internal Auditors. Thoughtful AI prompts define an audit's objective, scope, inputs, and constraints to focus analysis on relevant information and evidence. This tool will help auditors develop structured prompts that produce precise, consistent outputs aligned to the audit's scope and objectives.

TOOLS

AI Governance Best Practices. Data governance is often messy in organizations, complicating audit procedures. This tool will help auditors assess the structure, design, and operating effectiveness of AI governance.

GLOBAL PRACTICE GUIDE

Assisting Small Internal Audit Functions With Implementing the Standards will highlight common implementation challenges, including independence safeguards, resource constraints, access to specialized expertise, quality assurance, and stakeholder expectations.

community

Highlights

Bahamas Chapter Celebrates 35 Years

The IIA–Bahamas Chapter marked its 35th anniversary with a cocktail event and awards ceremony in May at Balmoral in Nassau. With the theme "Celebrating Impact: Honoring the Past, Inspiring the Future," the ceremony recognized five members for their contributions to the profession:

- **Kendra Culmer**, Commonwealth Bank Ltd. — Distinguished CAE of the Year.
- **Jamaice Rolle** — Distinguished Internal Audit Manager of the Year.
- **Alicia Smith**, Colina Insurance Ltd. — Distinguished Senior Internal Auditor of the Year.
- **Machara Tucker**, Colina Insurance Ltd. — Distinguished Internal Auditor of the Year.
- **Dinaj Major** *(not pictured)*, Risk Advisory Co-Op, Deloitte — Emerging Leader of the Year.

IIA–Croatia Turns 20

IIA–Croatia celebrated its 20th anniversary during its 15th annual international conference at Hotel Pinija in Petrčane. The April event welcomed nearly 200 participants from 15 countries, with keynote speakers Massimiliano Turconi and Liz Sandwith.

Before the conference, IIA–Croatia hosted a Central and Eastern Europe IIA meeting, attended by representatives of 12 countries and ECIIA CEO Rachel Barlow. In May, institute members appeared on a radio station at the University of Zagreb, promoting the internal audit profession to students.

Career Moves

Sherry McLendon, CIA, CRMA, CHIAP, member of the IIA–Baltimore Chapter and an honorary 40-year IIA member, recently retired as senior internal auditor at Johns Hopkins University.

Hassan Khayal, DBA, CIA, CRMA, CFE, chief internal auditor at the Mohamed bin Zayed University of Artificial Intelligence in the United Arab Emirates, has been elected chair of the IIA Global Guidance Council. He is a member of IIA–UAE and a 2020 *Internal Auditor* Emerging Leader.

Eric Wilson, CIA, director of internal audit and CAE at Gulfport Energy and a member of the IIA–Oklahoma City Chapter, received *Internal Auditor*'s 2026 John B. Thurston award for best article published in the magazine in 2025. He recently joined the IIA Global Guidance Council.

Submit Your Achievement or Event to Trinity Spearman
Trinity.Spearman@theiia.org

Calendar

AUG 31–SEPT 1
Financial Services Exchange
Brooklyn, N.Y.

SEPT 8
ERM Virtual Conference

SEPT 14–27
In-Person IIA Learning Seminars
Washington, D.C.

OCT 1–2
Virtual COSO Fraud Risk Certificate
Developed by COSO with ACFE.

OCT 5–7
Canadian National Conference
Vancouver

OCT 29–30
AI Coordinated Assurance Certificate Program

NOV 2–3
IGNITE Conference
Washington, D.C.

IAm *Perla Habchi*

stats

CIA

Audit Manager /
Wealth One Bank of Canada

IIA–Ottawa Chapter /
Chair of Academic Relations /
Member since 2019

2024 *Internal Auditor*
Emerging Leader

I have always been drawn to creative work — whether it is sewing, drawing, cooking, photography, or styling fashion and interiors. Over time, and with the encouragement of those who raised me, these interests grew into lifelong creative passions.

At eight years old, I begged my grandmother to teach me how to sew. I watched her turn extra fabric into aprons, hem pants, and alter clothes. After my first sewing lessons, I made fabric dolls with matching outfits.

As I grew older, those skills stayed ingrained in me. Even today, you'll find me hemming a random pair of pants over lunch, altering clothing to give it new life.

Growing up with a deep fondness of detail and creativity better prepared me for a career in internal auditing in ways I never expected. Sewing taught me to notice small imperfections, solve problems thoughtfully, and appreciate that even the smallest details can make a meaningful difference.

Introducing

IIA Global Internal Audit Quality Certification

Flash your seal of quality.

Earning the IIA Global Quality Certification isn't just compliance — it's recognition that your department operates at the highest global standard, validated by the profession's most experienced assessors.

Be globally recognized. Request an EQA today. • *theiia.org/Quality*

IIA Quality Services

Preserve the Past.
Fund the Future.

For 50 years, the Internal Audit Foundation has strengthened the profession through research, education, and global support. Join us in celebrating this milestone by giving "$50 for 50 Years" and helping build the next half century.

DONATE $50 FOR 50
theiia.org/Foundation

Internal Audit
FOUNDATION
1976-2026

CUTTING-EDGE RESEARCH | ACADEMIC PROGRAMS | TALENT PIPELINE