internal auditor

JUNE 2026
A PUBLICATION OF THE IIA

BETTER TOGETHER

How AI is unifying assurance in organizations.

Empowering the Future

Meet The IIA's North American Chair

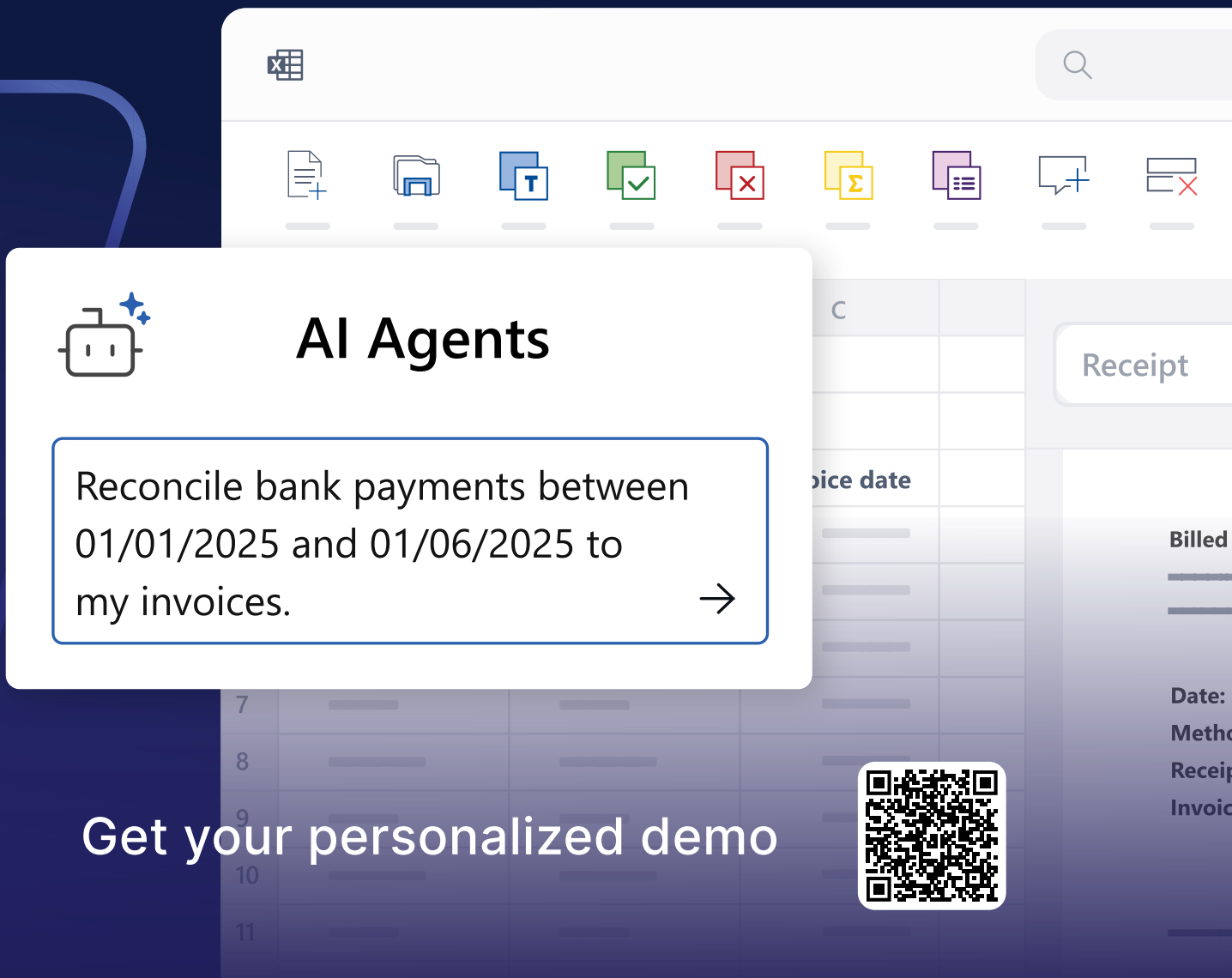
Top Teams

What makes the best audit functions so effective?

datasnipper

Turn complex testing into confident decisions.

Let AI Agents handle the heavy lifting inside Excel.



Get your personalized demo

Wolters Kluwer

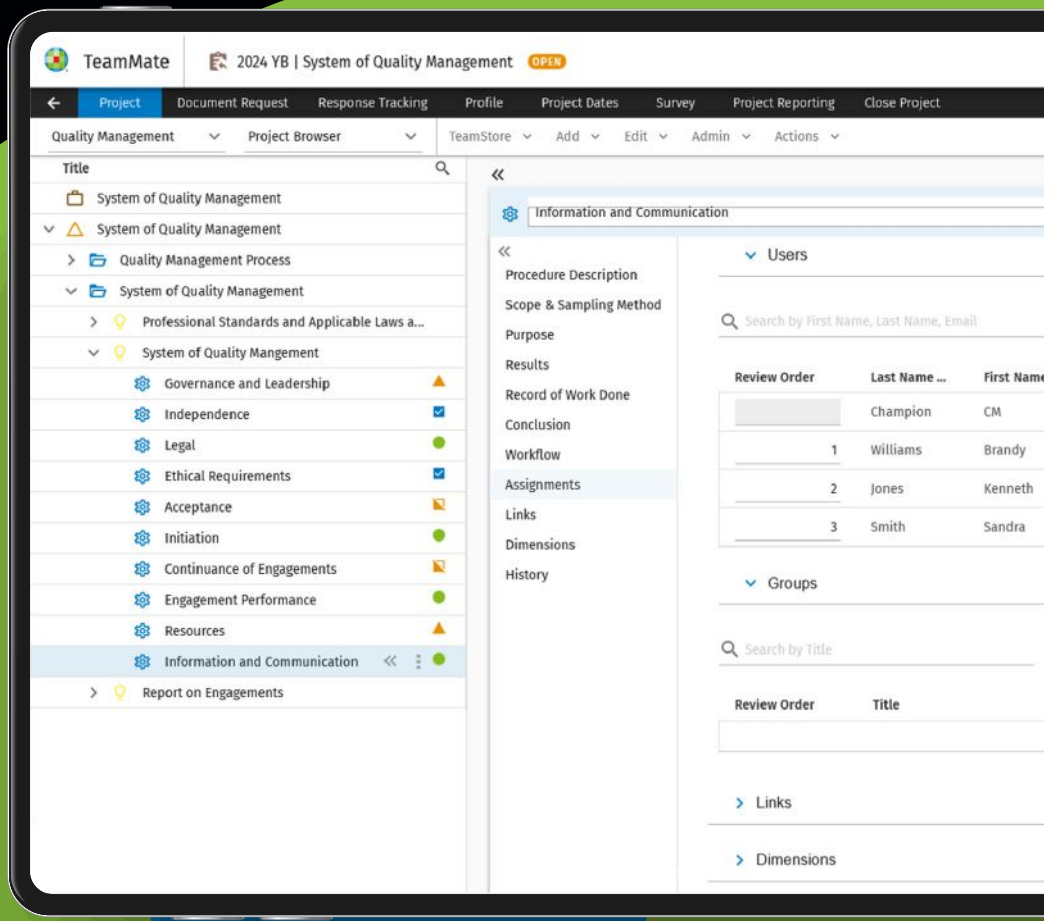
TeamMate®

Expert solutions for
stronger enterprise resilience

TeamMate Audit and GRC Software

Meet TeamMate at **Booth C07** at **IIA International Conference 2026** in Singapore to learn how leading organizations are strengthening enterprise resilience without the complexity of traditional GRC platforms

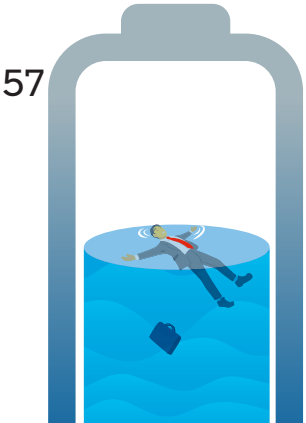
Register for our upcoming webinars



contents

featuring

departments



Transform risk into opportunity.

Supercharge internal audit with agentic AI.

Visit our booth to learn how.

GRC Intelligence → only at optro.ai

Optro

CE message

Celebrating **85 Years** of The IIA

I am honored to celebrate an exciting occasion this year: the 85th anniversary of The IIA. This moment offers an opportunity to reflect on how far the profession has come and recognize the global community that continues to shape its future.

Since its founding in 1941, The IIA has been guided by dedicated staff and volunteer leaders in its mission to support and advance internal auditing around the world. From establishing standards and guidance to delivering education, certifications, and thought leadership, The Institute has helped define what it means to be an internal auditor.

Over the decades, key milestones have marked The IIA's progress. In 1978, the introduction of standards for the internal audit profession — now known as the Global Internal Audit Standards — established a foundation for consistency and professionalism. In 1999, the Professional Practices Framework provided a more comprehensive structure for guidance, and in 2009, the addition of "International" underscored the global reach of our Standards and resources. More recently, enhancements to the IPPF, including topical requirements, reflect our continued commitment to providing focused guidance on increasingly complex risk areas.

This year marks another important achievement: the 50th anniversary of The Internal Audit Foundation. Through its forward-looking research and academic programs, the Foundation continues to help internal auditors anticipate emerging risks while preparing the next generation of talent.

The IIA's global impact is further reflected in the growth of the Certified Internal Auditor (CIA) designation. What began in 1974 with just over 600 CIA candidates has grown into a globally recognized credential held by more than 220,000 professionals.

The growth of The IIA community tells a powerful story about the profession, itself. What began in 1941 with just 84 members has grown into a global network of over 265,000 internal auditors across 170 countries and territories. This remarkable expansion reflects the rising demand over many decades for reliable, independent assurance and insight. Today, internal auditors work in organizations of every size and sector, bringing consistency, professionalism, and a commitment to strengthening governance and protecting value.

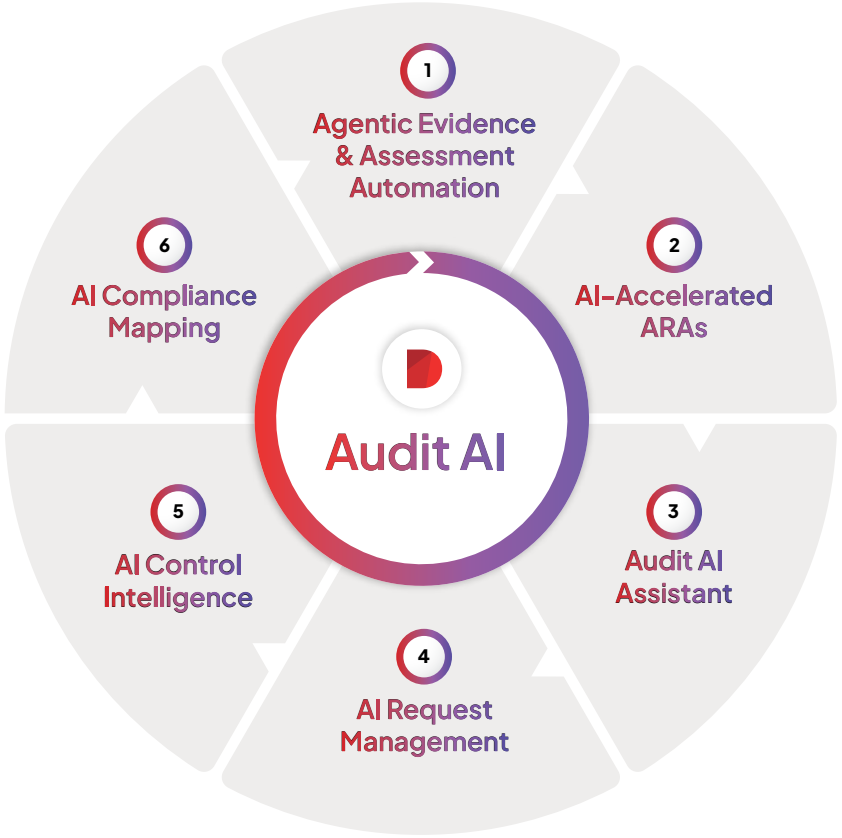
As we celebrate these milestones, we also look ahead. The challenges facing organizations are rapidly evolving, making the role of internal auditing more important than ever. Together, we will continue advancing the profession and advocating for the essential role internal auditors play in strengthening effective governance, risk management, and internal controls.

Anthony Pugliese

Diligent

Detect early.
Deliver certainty.
Only with Diligent Audit AI.

Surface emerging risks, automate evidence collection and standardize execution with agentic AI purpose-built for internal auditors. Deliver faster audits, stronger defensibility and clearer insight that leadership can trust.



With the only AI platform connecting audit with enterprise risk and compliance.

Diligent.com/AuditAI

editor's note

Let's Collaborate

Producing a magazine is all about collaboration. For each issue of *Internal Auditor*, our editorial team finds, edits, and compiles articles from more than a dozen practitioners, freelancers, and staff writers. While that's happening, our designers are working with artists and photographers to produce the incredible art for those stories.

Meanwhile, content producers are developing podcasts to build on those articles, and the sales and marketing teams are developing ads. And, when the issue is ready, the magazine goes to our printer, digital platform, and web and social media teams to deliver it to IIA members across all our channels. None of it happens without constant collaboration.

When I started my career in journalism, there were lines we didn't cross. Magazines and newspapers were print, while television and radio delivered news through video and sound. There was a strict wall between advertising and editorial. Now, the editorial wall is mostly gone, and all types of media produce articles, videos, and podcasts across every platform possible.

Internal auditing is having that type of moment today. In many organizations, the three assurance lines are coming together and, in some cases, becoming intertwined. Globally, 32% of internal audit function leaders oversee or are responsible for at least one second-line assurance function, according to the Internal Audit Foundation's recent Collaboration Without Compromise report. The Foundation worked with Baker Tilly and Wolters Kluwer on the survey of 3,000 internal audit and risk practitioners.

The report notes this collaboration among the lines is expected to deepen — and in 39% of respondent organizations, it already has. Survey respondents say it has improved risk coverage, reduced duplicate efforts, and strengthened alignment.

In our June cover story, "Better Together" (page 22), we explore how artificial intelligence (AI) can help internal audit work more closely with other lines of assurance. AI-driven combined assurance can connect systems and processes, while automating how teams coordinate work. That can enable internal audit and second-line functions to focus on "judgment-intensive work," writes Ashwathama Rajendran, data analytics lead for financial technology company Stripe.

AI could bring the three lines into closer collaboration, much as the internet brought down the many walls in the media world.

TimMcCollum10

internal auditor

JUNE 2026

EDITOR IN CHIEF
Tim McCollum

MANAGING EDITOR
Jake Lamb

SENIOR EDITOR
Christine Janesko

ASSISTANT EDITOR
Trinity Spearman

STAFF WRITER
Logan Wamsley

ART DIRECTION
Em Agency

CONTRIBUTING EDITORS
Steve Mar, CFSA, CISA
Dan Ramey, CIA, CRMA, CPA, CFE
James Roth, PHD, CIA, CCSA, CRMA
Rachel G. Brueggen, CIA, CRMA

GLOBAL CONTENT ADVISORY GROUP
internalauditor.theiia.org/en/about/staff

EDITORIAL
jacob.lamb@theiia.org

ADVERTISING
advertise@theiia.org

SUBSCRIPTIONS, CHANGE OF ADDRESS
customerrelations@theiia.org

PERMISSIONS AND REPRINTS
copyright@theiia.org

WRITER'S GUIDELINES
internalauditor.theiia.org

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

A PUBLICATION OF

The Institute of Internal Auditors

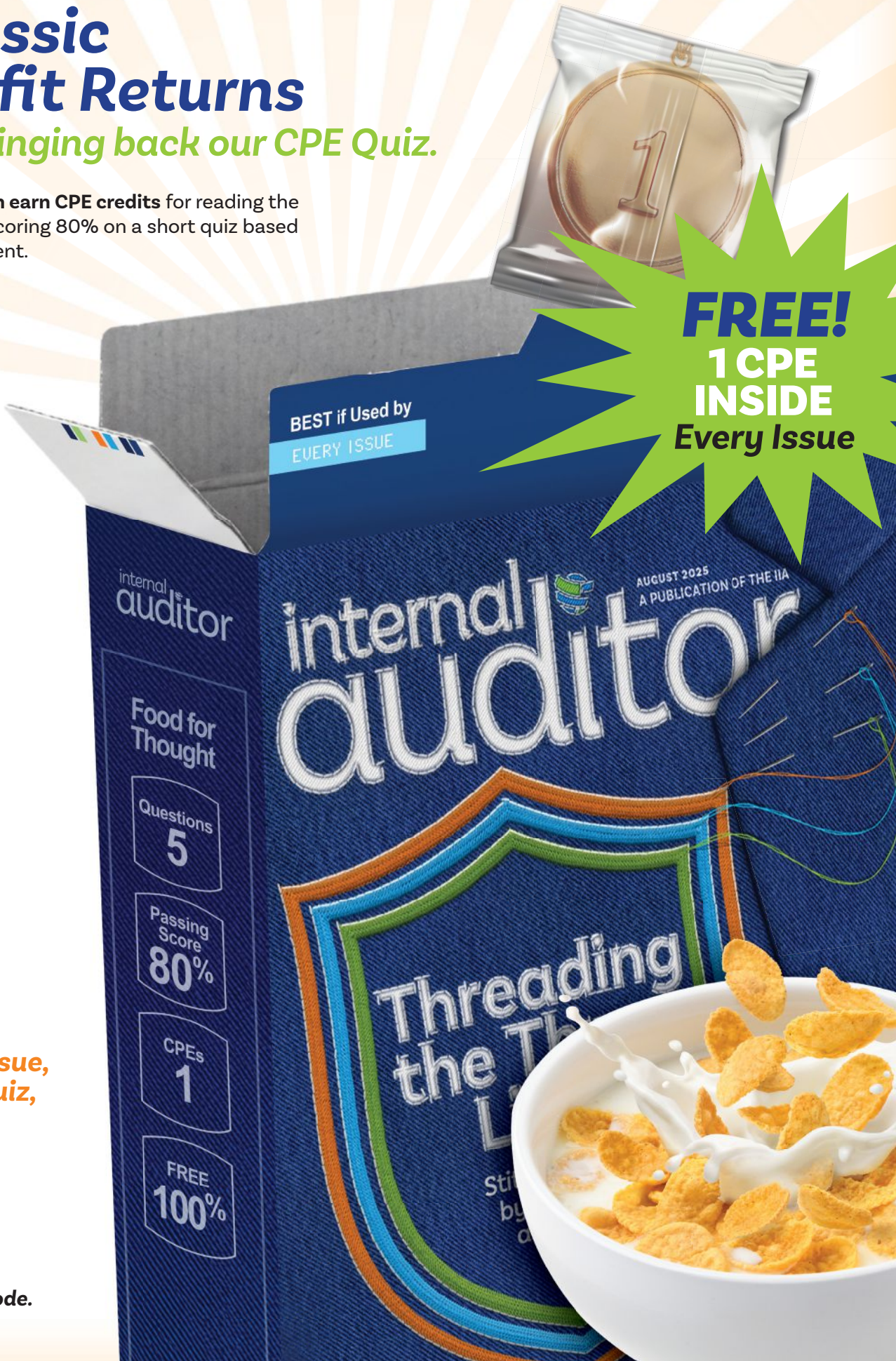
PRESIDENT AND CEO
Anthony Pugliese, CIA, CPA, CGMA, CITP

CHAIR OF THE BOARD
Stefano Comotti, CIA, CRMA

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.

update

Modernizing Sarbanes-Oxley

The IIA urges lawmakers to recognize internal auditing's compliance role.

More than two decades after the U.S. Sarbanes-Oxley Act of 2002 was enacted, an IIA public policy paper calls on lawmakers to modernize the law and integrate internal auditing into its framework.

One way to do this is to include a legal definition of the internal audit profession's role in Sarbanes-Oxley compliance, which the law currently lacks. That lack of clarity about internal audit's role can lead to inefficiencies and unnecessary costs, the paper notes.

The public policy paper also recommends that the U.S. Congress re-examine the work needed to comply with Section 404 Internal Controls Over Financial Reporting and Section 302 Executive Certifications Assurance. The burden of Sarbanes-Oxley compliance is "heavy and growing," said Lawrence Cunningham, director of the University of Delaware's John L. Weinberg Center for Corporate Governance, in testimony before the House Financial Services subcommittee in June 2025.

"Policymakers and governance leaders have an opportunity to ensure the law continues to protect investors and strengthen financial markets while also promoting greater efficiency and reducing unnecessary compliance burdens," says IIA President and CEO Anthony Pugliese in a press release.

The compliance workload has particularly impacted internal audit functions, the IIA paper adds. According to KPMG's 2025 SOX Survey, 52% of internal audit departments dedicated more than 40% of their total hours to Sarbanes-Oxley compliance in 2024.

The paper's other recommendations include:

- Strengthening partnerships between internal and external auditors.
- Reducing compliance costs by using technologies such as artificial intelligence and continuous monitoring.
- Giving internal audit a voice in regulatory policy discussions and ensuring that stakeholders understand the profession's value in protecting investors and markets.

To that end, the paper cites benchmarking data from 158 publicly traded companies that shows 91% spend less than 0.8% of revenue on internal audit. — *Trinity Spearman*

HIDDEN TAX ON ENTREPRENEURS

Every year, cybercrime costs U.S. small businesses

$131 BILLION

72% OF SMALL BUSINESSES were hit by fraud, scams, or ransomware in 2025.

71% OF SMALL BUSINESS OWNERS say they fear AI will make fraud and ransomware attacks more frequent.

Businesses lose about **$60,000 per incident** of payment fraud and email phishing.

SOURCE: PUBLIC PRIVATE STRATEGIES INSTITUTE, FRAUD, SCAMS, RANSOMWARE: SMALL BUSINESSES REACT

Global Unrest

Supply chains strain as energy risks and geopolitical uncertainty rise.

According to recent surveys, global business leaders entered 2026 on relatively solid footing. Yet, that confidence has waned quickly as geopolitical tensions have escalated, disrupting supply chains and driving renewed concern over energy costs.

Findings from the latest McKinsey Global Survey show how fast sentiment has shifted. Executives echoed a more positive tone at the end of 2025, but after late-February, tensions in the Middle East have fueled concerns about geopolitical instability. Nearly three-quarters of respondents now view it as the top global risk, a sharp increase from 51% in December. At the same time, worries about energy prices (32%) tripled and supply chain disruptions (25%) doubled, with both emerging as leading threats to economic stability.

Concern about supply chains is even more pronounced among chief financial officers (CFOs). In Deloitte's recent CFO Signals Survey of 200 North American CFOs, 52% say they now see supply chain disruption as their top external concern, up from 35% in the previous quarterly poll.

At the company level, CFOs are prioritizing resilience. According to Coupa's Strategic CFO Report, 600 finance chiefs from eight countries rank building stronger supplier relationships as the top strategic priority for 2026, ahead of technology concerns like artificial intelligence and cybersecurity.

Many business leaders are responding to supply chain concerns by strengthening collaboration. In a recent World Economic Forum survey, nine in ten executives say fostering international cooperation among organizations and governments to manage supply chains is critical to long-term success. According to the poll of 150 global business leaders across 12 countries, 80% say they are willing to deepen cross-border partnerships. *— Jake Lamb*

BOARD PRINCIPLES

New COSO guidance outlines 12 principles to strengthen board oversight.

"In today's environment, governance is a strategic capability. As boards navigate accelerating change and expanding risk, strong oversight is essential to sustaining performance and long-term value."

Ray Garcia, leader of PwC's Governance Insights Center, commenting on COSO's Corporate Governance: Guiding Principles for Board Oversight

COMPENSATION EXPECTATIONS

A survey of 1,000 U.S. employees and 500 employers reveals gaps in trust over pay — and suggests that better communication may improve retention.

93%

OF EMPLOYERS say their employees trust their pay decisions; 69% of employees agree.

63%

OF WORKERS paid at market rate say they are underpaid, and **47% of those paid above market rate** say the same.

72%

OF EMPLOYERS report an increase in salary negotiations driven by employee searches of sources such as Reddit, social media, and generative AI, which may offer unreliable data.

SOURCE: PAYSCALE, 2025 FAIR PAY IMPACT REPORT

ASK AN EXPERT

Water Woes

Arleen McGichen, MCIBS, CMIIA, is group chief audit officer for Royal London Group and president and director of the Chartered Institute of Internal Auditors for the U.K. and Ireland. She is based in Glasgow.

Why are U.K. internal auditors concerned about water utilities?

Late last year, well over 20,000 customers in Kent and Sussex counties had severe and prolonged water supply outages lasting several weeks. The failure occurred at South East Water, a privatized water utility that serves about 2 million customers. You can imagine the disruption to daily life, local businesses, schools, and — worryingly — hospitals and care homes. In April, there was a shorter outage affecting about 6,000 people. In 2022, there was one for over 23 days.

Because of that, there has been a renewed scrutiny on utilities' leadership, governance, and oversight by the Chartered Institute of Internal Auditors. In the U.K., for sectors outside of financial services — particularly the utility sector — there's no regulatory requirement for there to be an internal audit function or an established internal audit system within an organization.

We wrote to the U.K. water minister to raise our serious concerns about South East Water not operating with a more established internal audit arrangement and, particularly, without an in-house internal audit function.

What are the risks involved when utilities lack oversight?

Water is such a critical part of the nation's infrastructure. When the supply fails, it has a ripple effect on other sectors and other industries being able to maintain their resilience. There are also cybersecurity and technological risks because a lot of our mainframe systems rely on cooling systems to prevent them from overheating.

So, we've effectively said to the U.K. government that it should introduce a legal or regulatory requirement for water companies in England and Wales to have an internal audit function. We think regulators should publish clear guidance stating that internal audit is an essential part of good governance and a best practice for water companies.

We're not saying that internal audit is a silver bullet to the operational and financial issues facing the water sector. But the lack of access could mean that the boards of these companies are not getting sufficient independent assurance on their business-critical risks.

Water is such a critical part of the nation's infrastructure. When the supply fails, it has a ripple effect on other sectors and other industries being able to maintain their resilience.

AGENTS OUTPACE OVERSIGHT

AI agent adoption is accelerating faster than governance readiness, IT and business leaders say.

21%
say their organization has a mature governance model for agentic AI.

ABOUT 80%
lack core safeguards such as decision boundaries, real-time monitoring, and audit trails.

74%
expect at least moderate use of AI agents by 2027, with 5% expecting full integration into core operations.

SOURCE: DELOITTE, 2026 STATE OF AI IN THE ENTERPRISE

Auditing Public Projects

Early-cycle audits can help keep bond-funded construction projects from snowballing into costly problems.

Erik Clarke

Capital construction programs rarely fail late. They start snowballing during scoping, contracting, early pay applications, or detailed requests for vendor payment. Those small deviations compound into delays, change orders, and budget overruns.

The most valuable public sector bond program audits happen early in the project. Early-cycle audits require disciplined scoping, a short list of risk signals, and testing, while there's still time to correct course.

An early construction audit needs to answer three questions: Does the scope align with what is being built? Are financial controls, such as contingencies, allowances, and pay applications, structured to prevent leakage? Do change orders have reasonable governance controls?

10 Critical Tests

Bond packages often include multiple projects, so internal audit should start with a small, early-stage subset. Auditors should gather scoping paperwork (contract and planning estimates), the procurement file, the executed contract documents, the first few pay applications, and logged change orders. Next, they should identify operational owners and the financial point of contact.

During the course of a construction project audit of a bond package, audits should be iterative and test different phases of the project. Each test outlined in this article uses documents most governments already keep. These tests are practical and timely.

1. Scope Discipline. Auditors should confirm that what voters and governing bodies approved aligns with the executed project scope and that changes are governed, not improvised.

How to Test: Internal auditors should reconcile the approved scope to the contracted scope of work with the construction vendor and the specifications. They should determine the scope creep, or the expansion of project requirements, and search for features that were not approved but are now standard.

Signs of Problems: Vague scope statements, missing traceability to voter language, and additional consultant or subcontracted work now in scope.

The most valuable public sector bond program audits happen early in the project. Early-cycle audits require disciplined scoping, a short list of risk signals, and testing, while there's still time to correct course.

2. Estimate Transparency. Internal audit should validate that early cost estimates are based on documented quantities and market-aware assumptions.

How to Test: Auditors should request the estimation basis for budgeting, including quantities, unit rates, escalation, productivity, and contingency.

Signs of Problems: Rounded number allowances, escalation not tied to a source, estimated materials or labor below market rates, and productivity assumptions copied across different sites.

3. Contingency Architecture. Internal audit should ensure that contingencies

are appropriately sized based on the total cost of the project and used to address unknown factors, not subsidize scope changes or underbidding.

How to Test: Auditors should identify owners, design, and other contractor contingency reserves for different components of the project, and their authorized uses. They should sample drawdowns in contingency reserves from the first few months, then tie each to allowed purposes using underlying documentation.

Signs of Problems: Contingencies are funded for clearly foreseeable reasons, contingency draws have minimal supporting documentation, and there is no forecast for remaining risk.

4. Allowance Clarity and Depletion. To help prevent allowance drift, auditors should examine whether vague allowances mask scope gaps.

How to Test: Auditors should list contract allowances and intended uses for those allowances, track drawdowns in the project reserve, tie to the material quantities that have been installed and unit costs, and verify reconciliation back to the contract sum.

Signs of Problems: Nonspecific allowance language, heavy draws without quantity reconciled, and no adjustment to contract sum when allowances are resolved.

5. Pay Application Anatomy. Internal audit should verify whether the first pay applications set the right habits for quantity verification and funds held back until completion (retainage).

How to Test: Auditors should trace sample line items from the schedule of values — an itemized document breaking down the contract — to field quantity verification, unit pricing, retainage math, and the payment approvals.

Signs of Problems: Unreasonable percentage complete with no field notes, percentage complete with field notes that don't align with the percentage, stored materials billed without proof of title and insurance, and retainage that is inconsistently applied.

6. Labor and Burden Reasonableness. Audits should aim to detect whether the size of overhead management is appropriate early in the project life cycle.

How to Test: Auditors should review a sample of time cards and burden rates (total indirect costs) for field supervision and general conditions. They also should compare labor hours to contract caps and industry norms. In addition, they should check for double-counted costs such as vehicles charged both as an allowance and a burden, resulting in duplicated costs.

Signs of Problems: Burden percentages applied to non-labor expenses and field supervision billed above agreed caps.

For each finding, internal auditors should state the control objective in plain language and summarize what was tested and what was found.

7. Change-order Controls. This test should help the organization prevent change orders from bypassing governance controls to protect the project's scope, schedule, and budget.

How to Test: Auditors should examine the first change-order proposal, including origin (owner or discovery), pricing basis (unit rate or time and materials), and approval path. From there, they should confirm that proposals route through the contractually required procedure (design review, independent cost estimate, and board approval).

Signs of Problems: Field directives become the de facto change-order source, time and materials pricing is used without appropriate reconciliation, and approval thresholds are not adhered to.

8. Schedule Realism and Float Protection. This test is intended to help the organization prevent early slippage, or the project getting behind schedule, from creating necessary change orders.

How to Test: Auditors should review the baseline

schedule and the first update. They should check float consumption to date, or the amount of slack time allocated to different phases of the project, and productivity assumptions. Moreover, they should verify that owner decisions and submittal cycles are represented in the schedule with realistic durations.

Signs of Problems: Critical activities with open ends, float burned in early project stages, and unrealistically short owner review cycles.

9. Procurement Integrity. Internal audit should confirm that the path from the request for proposal to awarding the construction contract aligns with the organization's policy and produced a competitive bidding process.

How to Test: The audit should reconstruct the bidder short list and scoring, review conflict of interest disclosures, sample communications during the procurement window, and tie selection criteria to documented strengths and weaknesses in winning and losing bids.

Signs of Problems: Missing or incomplete scoring sheets, narrative justifications that don't match scores, and default vendor language in the documentation.

10. Public Reporting. Auditors should evaluate whether the program's external dashboard and reporting are accurate, comprehensive, and useful to taxpayers.

How to Test: During the audit, practitioners should compare the current public report to project reality, including budget-to-actuals, contingency and change-order summaries, and schedule variances and cause disclosures.

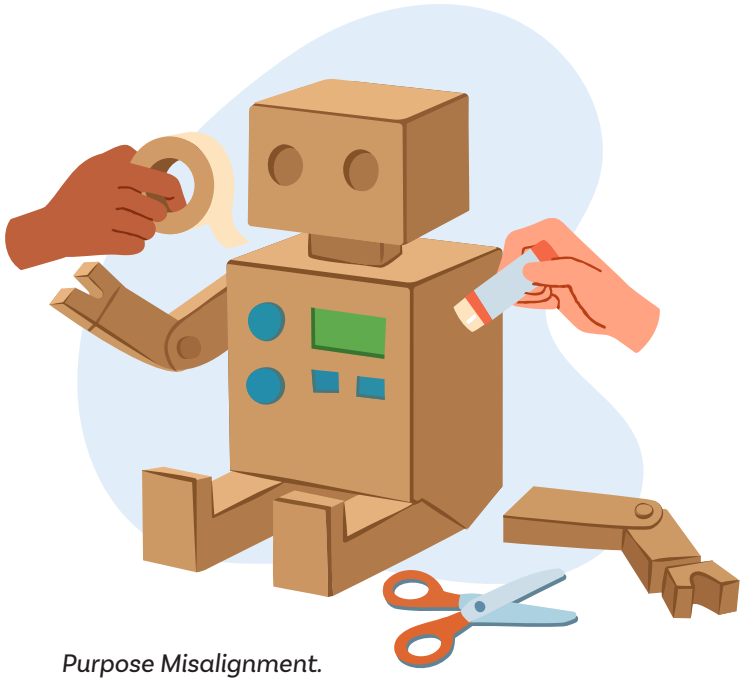
Signs of Problems: Dashboards built from milestones rather than cost or schedule documentation, variance narratives that blame market conditions without specifics, dashboards that omit information, and dashboard reporting that does not reflect underlying documents.

Driving Change

Early-cycle construction audit reports prevent issues, rather than just report findings. For each finding, internal auditors should state the control objective in plain language and summarize what was tested and what was found. Based on that information, auditors should recommend an adjustment that can be applied immediately and suggest a structural adjustment that can prevent the finding from recurring. This approach helps project teams move quickly and makes following up on findings more impactful.

Erik Clarke is the chief financial officer of a finance company based in Denver.

Assuring AI Success



Internal auditors must help ensure ambitious AI projects aren't built on a flimsy framework.

Israel Sadu

Transformative technologies often lead to exuberant, misaligned investments, and artificial intelligence (AI) is no exception. International Data Corp. (IDC) forecasts that global AI spending will reach $632 billion by 2028.

Amid this surge in spending, high-profile failures such as Volkswagen's Cariad software platform — which resulted in $7.5 billion in operating losses over three years before the project ended in 2025 — show how quickly ambition can outpace value. As organizations race to adopt AI, internal audit should ask: Are these investments delivering value for money?

For internal auditors, this question is about protecting shareholder value. A Massachusetts Institute of Technology survey, The GenAI Divide: State of AI in Business 2025, finds that 95% of AI pilot projects fail to deliver a return on investment (ROI). Just 13% of executives saw ROI from such initiatives within a year, according to a 2025 Deloitte report, AI ROI: The Paradox of Rising Investment and Elusive Returns.

The high failure rates and cost overruns point to the need for internal audit to assess AI projects for strategic alignment, risk exposure, and value realization. By understanding the common failure patterns, auditors can design assurance frameworks that help ensure positive ROI.

How Projects Fail

The causes of AI project failures are familiar, echoing the same pitfalls seen across technology initiatives.

Poor Governance. Just 8% of U.S. publicly listed companies disclose board-level oversight, and only 9% have established AI policies, according to a recent Institutional Shareholder Services (ISS) report, Mind the Governance Gap.

Purpose Misalignment. Business and technology teams often pursue different outcomes. IDC's CIO Playbook 2025 finds that 88% of AI pilots fail to reach production, largely because of unclear business objectives, insufficient data readiness, and gaps in technical execution. Without clear key performance indicators (KPIs) in the development process, projects suffer from fragmented collaboration and unclear or misaligned ROI objectives.

Poor Data Quality. High-quality data is the most overlooked pillar of AI success. According to a November 2024 *Forbes* article, "Why 85% of Your AI Models May Fail," AI models often fail because of bad data, underscoring the need for strong data governance and validation.

Cost Overruns. Many organizations underestimate the complexity of responsible AI deployment. A 2025 Benchmarkit and Mavvrik survey finds that 85% of organizations underestimate AI costs by more than 10%, and nearly one-fourth of them exceed budgets by over 50%. Unexpected costs often stem from core components such as data platform upgrades, integration challenges, and compliance overhead.

Get Involved Early

Internal auditors can support clients by participating in decision-making as advisors and observers, and by providing assurance through planned audits. As advisors, auditors can help assess AI strategy, governance, and human factors, according to The IIA's Artificial Intelligence Auditing Framework. Early internal audit involvement can help ensure that value assurance begins at the point of design and may include:

- Observing AI steering committees or planning sessions to understand the

initiative's scope, intended value, and risks.
- Reviewing documentation of AI use-case proposals to identify value alignment issues.
- Advising on governance structures by sharing insights learned from previous audits or industry benchmarks.
- Providing feedback on proposed value metrics and KPIs to ensure they are auditable and tied to business outcomes, without participating in performance-setting.

These activities help auditors challenge assumptions, assess readiness, and ensure AI initiatives are built for accountability and long-term value, without compromising their independence.

Focus on Value

By shifting from reactive control checks to proactive value assessment, internal audit can drive accountability. This role demands that auditors be fluent in technology, strategy, and human factors. To support value assurance, auditors should prioritize several areas during engagements.

Governance and Strategic Alignment. Despite rapid AI investment, board oversight of these projects remains limited. The ISS report notes that only 8% of U.S.-listed companies have board-level oversight of AI and just 16% have at least one director with AI expertise. Many boards defer AI oversight to technology committees or chief information officers, missing broader strategic governance implications that warrant direct board attention.

Internal auditors should check whether AI investments are clearly linked to strategic objectives and supported by measurable KPIs such as ROI, automation rate, and predictive accuracy. They also should verify that governance structures provide board-level oversight and are not siloed in the IT function.

Shadow AI, such as unvetted AI tools and third-party model add-ons, is creating a growing governance gap in many organizations. Auditors should identify and inventory any unapproved AI tools in use, assess their risks, and recommend they be brought under formal governance and control frameworks.

Organizational Readiness. AI success depends on data maturity, infrastructure, and internal capability. Auditors should evaluate data governance, accessibility, and readiness frameworks.

Performance and Ethical Use. Auditors should assess business outcomes such as productivity gains, cost and time savings, and customer retention, not just technical metrics like model accuracy. Clear baselines and business-linked KPIs are essential.

Ensuring ethical use can be easier said than done. In 2022, researchers at the University of Oxford in the U.K. observed a 12-month AI ethics audit at pharmaceutical company AstraZeneca, which revealed challenges in embedding ethics consistently across business units.

Cost Transparency. Data preparation and platform readiness are major cost drivers in AI initiatives. They account for roughly 30% to 50% of total budgets and 50% to 70% of overall project effort, according to Meta Intelligence's recent AI Project Cost Breakdown. Moreover, integration with legacy systems, model maintenance, and compliance overhead can distort ROI projections. Auditors must consider the total cost of ownership to provide a realistic view of value.

Scalability and Sustainability. Auditors must assess whether AI solutions are built for long-term use. This includes evaluating technical scalability, such as cloud capacity and modular design, as well as business adaptability. Sustainability also means planning for model updates, retraining, and governance, without which initial ROI may erode over time.

Key Takeaways

To help ensure AI projects deliver the most ROI, internal auditors need to be engaged early and assess whether initiatives are aligned with business objectives and governed effectively. Auditors should evaluate whether AI investments are positioned to deliver measurable and sustainable returns by asking:

- ***What is the business case for this AI investment?*** Internal audit should confirm the initiative supports a defined strategic objective and that expected benefits and assumptions have been validated with business owners, not just IT.
- ***How will success be measured and reported?*** Auditors should check whether there is a reporting mechanism to track performance against KPIs over time.
- ***What controls exist for bias, security, and compliance?*** Internal audit should confirm the organization tests AI for bias, protects sensitive data, and applies basic oversight.

Investing in AI is no longer optional for organizations — it's a strategic imperative. Internal auditors who embrace a proactive, value-focused approach to these projects can help safeguard investments and shape how organizations realize sustainable benefits from AI.

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

risk

Tracking Currency Volatility

Global expansion and geopolitical disruption have amplified often-overlooked currency risk.

Jesse M. Laseman

In today's volatile world, artificial intelligence (AI) and cybersecurity dominate the headlines, sometimes overshadowing more subtle risks. One such example is currency risk. Also known as foreign exchange (FX) risk, currency risk impacts organizations of all sizes and sectors. Rate swings can quietly increase costs, distort financials, and create real exposure by derailing strategy.

With the current level of geopolitical disruption, supply chain shifts, and market volatility, currency risk needs to be brought to the forefront. Like cybersecurity and AI, internal audit can help mitigate it by weaving currency risk into existing audits — bringing clarity to an area that is often overlooked.

The Rise of Currency Risk

In recent years, currency risk has grown more volatile and complex. The risk can be classified in three ways:

Transaction Risk. Exposure stemming from specific financial transactions, such as receivables or payables, is designated in foreign currencies. Transaction risk is the impact of exchange rate fluctuations on the value of these payments.

Translation Risk. This risk pertains to the consolidation of financial statements from foreign entities into the parent organization (the local currency). For example, if a U.S. organization converts a Canadian subsidiary's earnings from Canadian dollars to U.S. dollars, it may realize lower profits if the Canadian dollar weakens.

Economic Risk. A more long-term, abstract, and strategic concept, economic risk helps quantify how competitive an organization is in global markets as currencies shift in value. For example, a product priced last year might become too expensive if the rates change, producing a ripple effect across profits, cost, and the overall strength of the organization.

Why Currency Risk Has Grown

One of the biggest drivers of currency risk is global expansion. As companies scale and build relationships with customers and vendors across borders, they naturally become more interconnected with foreign currencies. As exchange rates are consistently changing by wider margins, the risk only grows.

Geopolitical instability and trade tensions have also made currency risk harder to manage. Conflicts, sanctions, trade talks, and other political updates affect operations.

A clear example is the Russian ruble in 2022. After Russia invaded Ukraine, the U.S. and European Union both imposed sweeping economic sanctions on Russia. The outcome was that investor confidence collapsed, foreign capital fled for other opportunities, and the ruble quickly dropped in value. To save the ruble from crashing, the Russian central bank sharply raised interest rates to stabilize the markets, also affecting the rate at which organizations borrowed.

In this example, two main currency risks are involved: transactional and translational. If an organization outside Russia was supposed to receive rubles, the currency's collapse would reduce the value of that payment (transaction risk). Similarly, if an organization had assets in Russia during this time, the ruble's drop would lower the value of those assets when reported in their home currency, affecting the perceived value (translation risk).

The ruble crisis in 2022 is a simplistic example of the impact of exchange rate changes. Both 2025 and 2026 have seen even more volatility because of the threat of new tariffs and reactionary counter-tariffs. For companies with international operations, this creates greater uncertainty about pricing, asset valuations, budgeting, and cash-flow planning.

Hedging Currency Risk

Controls regarding currency risk can be as diverse as the currencies involved. Companies can hedge against currency risk to reduce the

transactional and translational impact of exchange rate changes. Financial instruments, such as hedging contracts, or operational strategies like balance sheet matching are a few examples.

A hedging contract is an agreement, typically made with a financial institution, to reduce exposure to currency fluctuations by locking in an exchange rate. These contracts usually specify the currencies, exchange rate, amount, and settlement date when the parties exchange funds at the agreed rate. Internal auditors should address several controls related to hedging.

FX Risk Policy. As part of good governance, there should be a policy to define the organization's oversight structure, risk appetite, hedging objectives, and approved instruments, such as forwards, swaps, and options.

Exposure Monitoring and Escalation. The organization should have a formal process to identify, understand, and quantify currency risk exposures across the business. This is most easily done for each segregated business unit or geographic region. Reporting should be consistent (monthly or quarterly), with enterprise resource planning or treasury management system (TMS) tools in place to automate data capture, reduce errors, and support timely oversight. A TMS gives a clear view of where cash is held and how currency changes could impact the business, helping leaders make better decisions and identifying areas of risk and opportunity.

Hedge Execution and Documentation. Carrying out hedging transactions without a plan or defined policy creates exposure. Trades should be documented appropriately and comply with applicable accounting standards. Segregation of duties is essential — trade execution, approval, confirmation, and settlement must be handled by separate people or teams, with post-trade controls in place to confirm deals and ensure accurate settlement recording.

Counterparty Risk Management. Internal audit should consider counterparty risk in the same vein as vendor risk management. Every hedging contract has a second party, which carries risk of defaulting. The control for this is setting credit limits based on reviews and past agreement history. Credit conditions change fast, especially in volatile markets. Ongoing monitoring can help ensure the risk stays within acceptable limits.

Integrating Currency Risks

With planning, internal audit can provide assurance over the design and effectiveness of currency risk management. Even if currency risk is not explicitly included in the annual audit schedule, it can still be evaluated indirectly through other scheduled audits.

For instance, during an accounts receivable audit, the team can review whether the organization issues invoices in foreign currencies. If so, internal audit should check whether there are controls to track exchange rates between billing and payment. This can reveal exposure to gains or losses if receivables are not settled in a timely or protected manner.

Similarly, in accounts payable audits, practitioners can examine whether vendor payments made in foreign currencies are subject to pre-approval thresholds or exchange rate monitoring. If a U.S.-based organization pays suppliers in euros, audit testing might verify if the finance team is consulted on timing the payment to manage exchange rate risk, or if contracts or forward agreements lock in rates in advance.

In a third-party management review, especially involving foreign vendors or service providers, auditors can assess whether procurement and legal teams consider currency risk when negotiating contracts. Auditors should evaluate whether prices are fixed in the organization's base currency or if the organization is assuming currency risk without appropriate oversight. Testing might include reviewing sample contracts and determining whether FX-related terms are consistently applied and monitored.

Lastly, with inter-company transactions, internal audit can evaluate how exchange rates are applied in accordance with regulations and internal policies. This evaluation may include validating whether pricing between various entities aligns with currency risks.

Another step is evaluating whether the organization accurately records and reviews currency gains or losses. Moreover, auditors can assess whether centralized finance team functions effectively support subsidiaries in managing FX risks.

Keeping FX Risk on the Radar

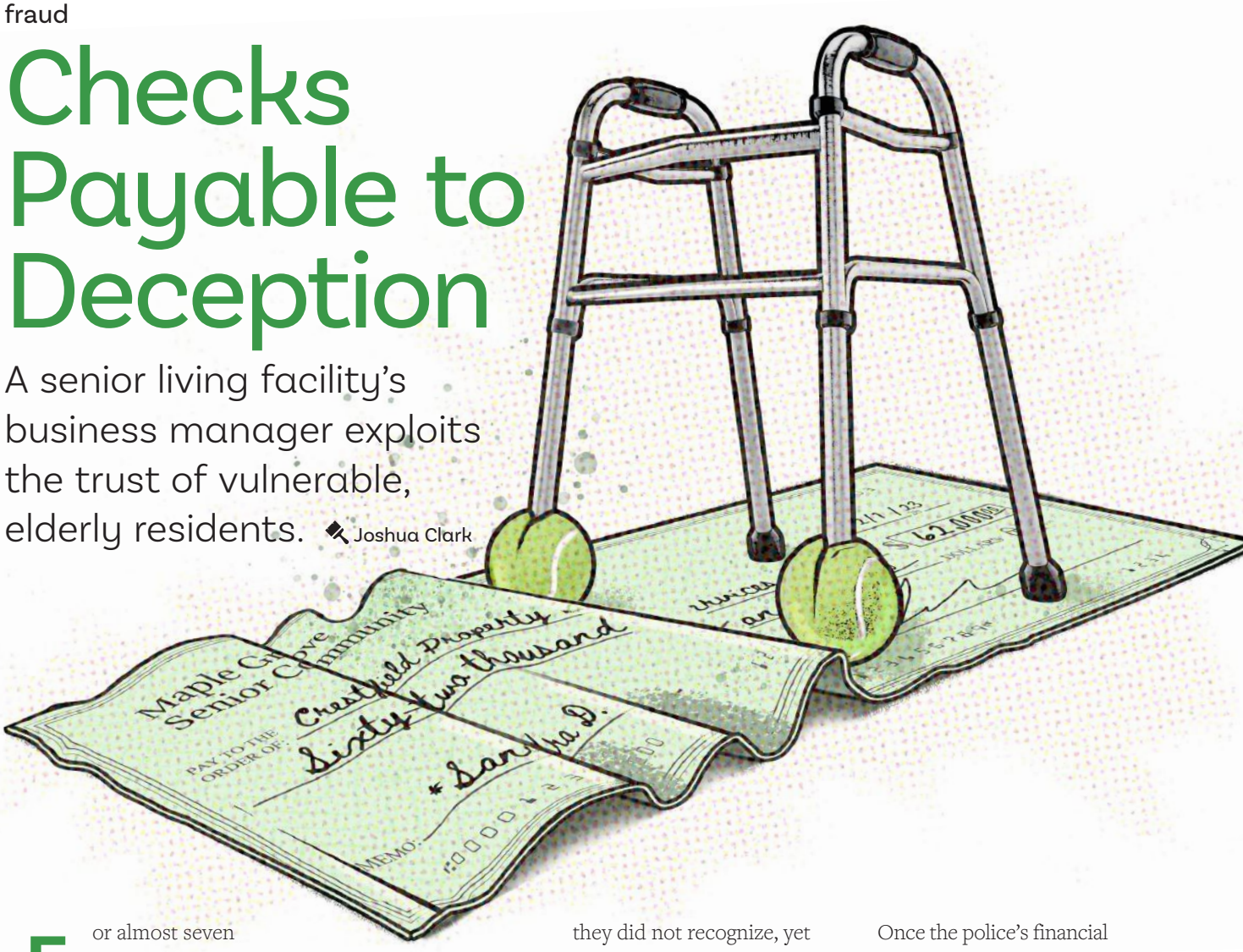
Amid geopolitical disruption, supply chain shifts, and ongoing market volatility, organizations must give currency risk increased priority and attention. It may not grab headlines like cybersecurity or AI, but rate swings can quietly increase costs, distort financials, and create real exposure by derailing strategy. This is where internal audit can add value. By integrating currency risk with existing audits, internal audit can ensure greater visibility and oversight.

Jesse M. Laseman, CIA, CRMA, CFE, is a senior internal audit consultant at Sikich in Naperville, Ill.

Checks Payable to Deception

A senior living facility's business manager exploits the trust of vulnerable, elderly residents.

Joshua Clark



For almost seven years, Sandra Daley seemed like the type of employee every senior living community wants: organized, approachable, and efficient. As the business manager at Maple Grove Senior Community — a memory care and assisted living facility — Daley was the financial face of the organization. She answered questions about billing, helped residents fill out paperwork, and knew almost every resident by name.

Daley had near-unchecked financial authority at Maple Grove. She was responsible for collecting rent, issuing billing statements, and being the primary point of contact whenever residents or their families had questions about charges.

Cracks in Daley's façade began to appear in early 2023. Two family volunteers, Margaret Holloway and Cynthia Marsh, began comparing notes after discovering unusual charges in their mothers' bank statements. Both found checks to a company they did not recognize, yet many of the charges were the same amounts as their rent.

The pair took their findings to the facility's executives. Maple Grove's initial investigation found similar charges involving 28 other residents and totaling about $62,000. It responded by hiring outside forensic experts to conduct a comprehensive review of the past five years of financial records. While that was in progress, the facility placed Daley on administrative leave, but she resigned a few days later.

Once the police's financial crimes investigators became involved, their forensic trail led straight to Daley. They discovered she was redirecting payments by instructing residents to make their monthly rent checks and money orders payable not to Maple Grove, but to Crestfield Property Services LLC. Because of her position of authority, residents and families didn't question the change. Many of them were told about it verbally during routine conversations in the hallway or at the facility's welcome desk.

Crestfield was registered to Daley's home address. When she received the checks there, she endorsed them, mobile-deposited them into her bank account, and reconciled the facility's records to conceal the shortfall. It was a brazen crime, investigators and prosecutors said. They said what made the scheme especially troubling was it deliberately targeted residents with dementia and other cognitive impairments, such as Holloway's mother.

Some residents, unable to recall whether they had already paid their rent, were guided by Daley into writing a second check, prosecutors alleged. Others, disoriented by changes in routine or unfamiliar paperwork, simply did what the person in charge of billing told them to do. "Daley took advantage of some of the most vulnerable victims in our community," said Henry Marquez, lead prosecutor with the Elder Abuse Unit for the district attorney's office.

The financial crimes unit determined that Daley had stolen payments from 104 residents or their designated family representatives. The total amount diverted exceeded $1.6 million, but forensic analysts later estimated the true figure could be as much as $2.5 million when duplicate and unreported payments were fully accounted for.

In December 2023, police arrested Daley and charged her with felony theft. At her plea hearing, prosecutors presented testimony from family members, facility staff, and Maple Grove's corporate representatives, who described the emotional and financial devastation the scheme had caused.

Daley pleaded guilty and was sentenced to 15 years in prison and ordered to pay more than $1.6 million in restitution. For its part, Maple Grove repaid impacted residents using insurance proceeds and corporate funds.

After Daley's conviction, Maple Grove overhauled its financial controls. The facility adopted a dual-authorization model for all resident billing, requiring a second employee to verify payment instructions before sending them to residents. It redesigned billing statements to clearly identify the payee entity and direct families to a corporate verification number. In addition, Maple Grove put formal escalation protocols in place so that any billing discrepancy raised by a resident or family member automatically triggers a review above the local business office level.

The changes addressed long-standing vulnerabilities, but questions remained about how a single employee had near-total control of residents' funds. As Holloway noted, "Why did it take me to find it, rather than the people who work here?"

Lessons Learned

Enforce segregation of duties and independent authorization over payment instructions. To reduce opportunity to commit fraud, no single employee should be able to change the payee, communicate payment instructions, receive payments, and reconcile accounts. The organization should require independent approval and documentation for any payee or remittance change.

Perform independent reconciliations with exception reporting. Someone outside the business office should reconcile resident subledgers to bank deposits at least monthly. The organization should require documented follow-up on exceptions — such as missing deposits, unusual payees, duplicate payments, and out-of-pattern amounts — to detect diversion early.

Require conflict-of-interest disclosures. To address corruption and concealment risks, organizations should require employees in financial roles to periodically disclose outside business interests. They also should perform checks to identify employee-controlled entities, such as beneficial ownership/address matches, among vendors and any entity receiving resident payments.

Provide an independent verification and reporting channel. Because many victims were cognitively impaired, they were dependent on Daley's instructions. A corporate verification number or portal would enable residents and families to confirm payee details, while a confidential reporting channel would allow them to voice concerns without going through the local business office.

Treat billing concerns as fraud indicators and escalate them promptly. Because tips are a leading fraud detection method, facilities should have a clear process to receive and review complaints from residents and families. That should include case-management steps for escalating issues above the facility level and tracking them to ensure they are resolved timely.

Implement role-based fraud awareness training. Facilities should train new and existing staff members to recognize common fraud schemes, behavioral red flags, and documentation standards. Also, they should learn how to verify payment instructions. This training should be paired with a culture that encourages employees to speak up when they see wrongdoing.

BETTER TOGETH

Artificial intelligence can connect people, processes, and data to power combined assurance.

Ashwathama Rajendran

ER

Fragmented assurance — where one function is unaware of the findings of another — creates risk blind spots. It can manifest like this: A bank's cybersecurity team identifies unusual activity in a payment processing system but classifies it as a low-severity technical anomaly. At the same time, the compliance function flags a spike in customer complaints related to unauthorized transactions, while internal audit documents control weaknesses in the same system during a routine review. Each function operates within its own silo, applying its own risk ratings and reporting on its own timeline.

Individually, none of the findings triggers escalation. Together, they reveal a systemic control failure that could result in significant financial loss, regulatory penalties, and reputational damage. This is the kind of problem that an integrated, combined assurance approach can solve.

Combined assurance has emerged as a key framework for coordinating risk management activities across organizational lines (see "Combined Assurance and the Three Lines Model" on page 25). The case for AI-assisted combined assurance is even more compelling. Traditional combined assurance faces persistent challenges: coordinating disparate teams, maintaining consistent risk definitions, ensuring quality across multiple assurance providers, and creating truly integrated assurance maps that keep pace with evolving risks.

Artificial intelligence (AI) offers a timely opportunity to strengthen the combined assurance model at scale through its ability to connect systems and processes. By automating coordination tasks that historically have required extensive manual effort, AI allows assurance professionals to focus attention on judgment-intensive work. AI can enhance combined assurance across five dimensions — assurance mapping, risk language harmonization, work quality assessment, continuous monitoring integration, and stakeholder reporting.

AI-ASSISTED ASSURANCE MAP

The assurance map — a structured, visual aid identifying monitoring activities, owners, and coverage gaps — is the cornerstone of combined assurance. However, traditional assurance maps can quickly become outdated as organizational risks evolve. Updating them typically requires manual input from multiple stakeholders across different functions and reporting hierarchies, which is both time-consuming and prone to error.

The challenge is compounded by a lack of shared resources and tools. Only about four in 10 organizations share methodologies, risk registers, or risk and control frameworks between their enterprise risk management (ERM) and internal audit functions, according to the Internal Audit Foundation's research report, Collaboration Without Compromise: Practitioner Perspectives on Internal Audit, Risk Management, and Governance Practices. Just one in four share risk management software. By the time a static map is refreshed, risks may have already changed, making the map more of a historical record than a decision-support tool.

AI-powered assurance mapping introduces continuous intelligence. AI agents can automatically scan audit plans, compliance reports, risk assessments, and monitoring activities across all three lines to identify coverage areas. Agents can detect overlaps and gaps in real time, alerting executives to blind spots before they materialize into incidents.

For example, an AI agent could continuously map internal control coverage against evolving regulatory requirements, instantly flagging when a new data privacy law creates an unmonitored risk in the existing audit plan. This eliminates the "jigsaw puzzle" effect of receiving conflicting reports from multiple teams, providing management and the board with a comprehensive, integrated view of risk grounded in real-time data rather than fragmented, dated perspectives.

A COMMON RISK LANGUAGE

A challenge in combined assurance is achieving a common understanding of risk definitions, severity levels, and impact assessments. Different teams often use inconsistent taxonomies, or categories of risk, making coordination difficult and potentially leading to conflicting messages to stakeholders.

In the Internal Audit Foundation report,

practitioners say a shared risk language, taxonomy, and methodological alignment are key elements that strengthen the effectiveness of assurance when integration is done well, while their absence is cited as weakening assurance quality. A single third-party vendor issue, for instance, might be categorized as *procurement risk* by internal audit, *regulatory risk* by compliance, and *supply chain risk* by operations. While these functions describe the same core concern, using disparate frameworks can create a fragmented view of the organization's risk exposure and make it difficult for leaders to prioritize remedies.

Historically, organizations have relied on fuzzy matching logic — algorithms that identify approximate rather than exact matches between terms — or labor-intensive manual techniques to maintain risk maps. These methods break down when terminology diverges or when new risk categories emerge.

AI can overcome these limitations by serving as a semantic translation layer. By analyzing risk terminology within the reports of all three lines, AI models can identify similarities between different risk frameworks. AI-driven risk classification systems can automatically tag and categorize risks using a unified taxonomy. Over time, the model learns from human corrections and evolving regulatory guidance, steadily improving accuracy.

AUTOMATED WORK ASSESSMENTS

Internal audit is responsible for quality assurance, even when relying on the work of other providers. However, verifying that second-line functions or external auditors meet the same standards demands considerable time and resources.

This challenge intensifies as the volume of assurance work grows, as organizations expand into new regulatory jurisdictions, and as regulators demand more rigorous documentation. In the Executive Knowledge Brief, Combined Assurance, The IIA cautions that relying on others' work can negatively impact internal audit's independence if the quality, objectivity, or risk perspective of those providers is not adequately assessed.

AI can help auditors by:

- Systematically evaluating assurance quality across all providers.
- Reading workpapers in context.
- Assessing whether the evidence presented supports the conclusions drawn.
- Verifying whether testing methodologies are proportionate to the risk being evaluated.
- Identifying coverage gaps relative to the defined audit scope.

This approach doesn't replace professional judgment — it extends internal audit's oversight capacity. AI acts as a first-level quality screen, freeing internal audit to focus on substantive issues. It also creates a consistent basis for showing regulators and boards that its reliance on other assurance providers is well-founded.

INTEGRATED MONITORING

The expanding second line now includes cybersecurity, data privacy, sustainability reporting, anti-money laundering, and other specialized risk functions. Each function generates a steady flow of monitoring data from security logs, privacy incident reports, emissions measurements, third-party risk assessments, and transaction surveillance alerts. Bringing these inputs together into a clear combined assurance view is difficult, particularly when assurance teams use differing data formats, reporting timelines, and risk rating scales.

The Collaboration Without Compromise report illustrates how much work remains. Few organizations conduct core risk activities jointly across internal audit and ERM. Most still perform these activities separately, sharing information only at the end of the process. As a result, organizations have more monitoring data than ever before but lack a unified view of risk.

COMBINED ASSURANCE AND THE THREE LINES MODEL

The IIA defines combined assurance as a coordinated effort in which internal and external parties align their activities to communicate risk management effectiveness, eliminate redundancies, and improve efficiency. Grounded in the Three Lines Model, combined assurance assigns risk ownership to first-line business functions, oversight to second-line functions, such as compliance and risk management, and independent assurance to internal audit. According to the Internal Audit Foundation's Collaboration Without Compromise report, 72% of organizations use The IIA's Three Lines Model to define roles between second- and third-line functions.

The need for combined assurance is increasing. Sixty percent of practitioners expect greater integration of risk and internal audit functions over the next five years.

The IIA will issue an updated Three Lines Model as a Statement of Position in July. The refreshed model emphasizes the benefits of collaboration, coordination, and reliance among the three lines and external assurance providers.

AI can connect findings across assurance providers to reveal patterns that siloed reviews miss. For example, it could link an increase in customer billing complaints to recent software updates and unresolved audit findings. This broader view can highlight systemic issues that require joint action by IT, finance, and internal audit, rather than isolated actions.

This creates "continuous combined assurance" — real-time integration of monitoring activities across all three lines. Rather than assembling a composite risk picture quarterly, the organization maintains a living view of its assurance posture that updates as conditions change, identifying emerging risks sooner and coordinating remediation efforts across functions in near-real time.

INTELLIGENT REPORTING

Combined assurance ultimately benefits boards and senior management that need integrated risk perspectives to make decisions. Yet synthesizing assurance results across multiple providers into coherent executive reporting remains a persistent challenge. Reports are often produced on different timelines, in different formats, and with different assumptions about materiality.

AI can generate integrated assurance dashboards that dynamically aggregate findings across all three lines, automatically identifying themes, trends, and emerging risks. If the board asks, "How ready are we for the new digital operational resilience regulations?" AI can synthesize reports from the cybersecurity team, along with compliance gap analyses and recent internal audit reviews. This turns a week-long manual data collection effort into one instant, unified assessment.

Beyond responsiveness, AI-driven reporting can introduce greater objectivity, reducing the risk of unconscious framing biases and ensuring that relevant assurance activities — including those with unfavorable findings — are represented in the executive view. However, human judgment and governance is needed to verify that reports generated by AI don't introduce their errors and biases.

KEY CONSIDERATIONS

While AI-enabled combined assurance offers significant benefits, realizing them requires deliberate planning across technology, governance, and organizational readiness. Three considerations are essential for internal audit leaders looking to move from concept to implementation.

Use a Phased Adoption Strategy. According to the Collaboration Without Compromise report, 40% of practitioners cite limited resources or competing priorities as the top barrier to collaboration, followed by differing objectives (34%), a lack of unified platforms (32%), and siloed processes (31%). A phased approach to AI-enabled combined assurance addresses these barriers sequentially.

Internal audit should begin by automating assurance mapping with a bounded use case that builds familiarity in a low-risk setting. Next, it should use AI to create a common risk taxonomy, leveraging early wins to secure stakeholder buy-in.

As confidence in AI matures, internal audit should integrate quality assessment and continuous monitoring. Finally, it should deploy predictive analytics and integrated reporting capabilities. Each phase should include defined success metrics and feedback loops so that lessons learned inform subsequent stages.

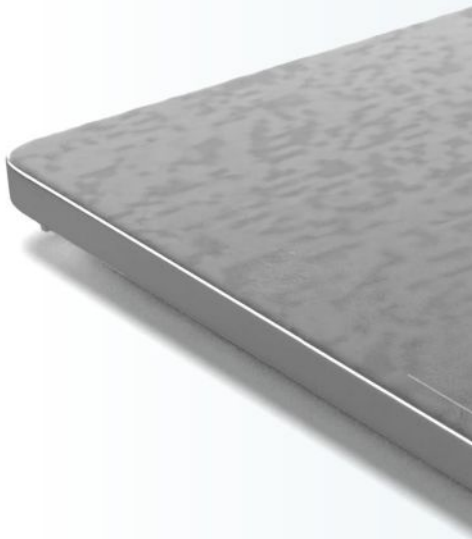
Apply Data Governance. Effective AI requires quality data governance, including standardized formats for risk and assurance information, clear data ownership across the three lines, data quality standards, and ethical AI principles over algorithmic decision-making. Without disciplined data governance, AI models will inherit the inconsistencies and gaps that currently hamper manual combined assurance, amplifying rather than resolving existing weaknesses.

Creating a cross-functional data governance committee with representatives from each line can help define common data standards and resolve disputes over data ownership.

Ensure AI Oversight. AI also introduces new risks that combined assurance must address such as algorithmic bias, hallucinations, and model opacity. The Three Lines Model provides a natural governance structure for these risks:

- First-line business units own AI systems as operational assets with accountability for their outputs.
- Second-line functions establish AI governance frameworks and monitor model performance.
- Internal audit provides independent assurance over AI risk management.

In this way, the combined assurance model becomes the mechanism for governing the technology that powers it. Early signs are promising. The collaboration survey found



that 80% of respondents saw no threat to internal audit independence from shared responsibilities between the second and third lines, indicating that deeper collaboration need not come at the cost of clear role boundaries.

STRONGER CONNECTIONS

Even with AI, the fundamental philosophy behind combined assurance remains unchanged — strengthening governance through collaboration while preserving independence. For audit functions, the opportunity from leveraging AI is clear: Transform from a periodic assurance provider to a continuous governance intelligence function that delivers real-time insights that impact decision-making.

Ashwathama Rajendran is a data analytics lead at Stripe in Boston.

Empowering the Future

The IIA's 2026-2027 North American Board Chair **David Helberg** says human capabilities will differentiate people from machines in the AI era.

Jason Cannon

The challenges of keeping pace with the latest advances in the machinery of business are nothing new. No industry or profession is immune. Certainly, changes in technology, communication, regulation, and governance have continuously shaped the internal audit profession over the past 100 years.

Today, we are witnessing the dawn of the artificial intelligence (AI) era, one that already is rapidly rewriting how business is done. I am not the first, nor will I be the last, to call on our profession to respond to this latest challenge with agility, creativity, and alacrity.

However, it will require more than simply understanding how best to leverage this new and powerful technology to set internal auditors apart. Indeed, the future of internal auditing will not be defined by the tools we adopt, but by the people we empower — their

judgment, confidence, and ability to turn uncertainty into insight. This is why I have chosen Empowering a Future-Ready Profession for my theme as the 2026-2027 North American Board chair.

During my term, the North American Board will champion this vision by working with IIA staff and volunteers to advance research, guidance, and talent development initiatives that strengthen both technological capabilities and the human judgment that differentiates internal audit. This work is essential to ensuring the profession remains relevant and positioned to deliver greater value in today's complex, AI-driven risk environment.

Internal Audit's Inflection Point

Less than four years since the introduction of OpenAI's ChatGPT large language model, AI has dramatically changed what stakeholders expect from internal auditors and how they define our organizational value. The profession is being asked to deliver strategic value in a more volatile environment with constrained resources.

A growing number of internal audit leaders report declines in both budget and staff in 2025, compared with the prior year, according to The IIA's 2026 North American Pulse of Internal Audit report (see "Pulse Trends" on page 31). The report urges practitioners "to carefully manage resources and demonstrate value to stakeholders by aligning with organizational strategy."

Responding to the AI challenge will take more than just a willingness to rethink our approaches to audit engagements or tweak our processes. Internal auditing isn't facing incremental change — it's at an inflection point. The question isn't whether expectations will keep rising; it's whether we're building the profession fast enough to meet those demands.

Driven by external volatility from AI disruption, geopolitical uncertainty, climate change, and other factors, boards and audit committees expect greater insight, faster reporting, and broader risk oversight from internal audit. Technology is transforming the profession, but tools alone are not the solution.

Across industries, technology is accelerating the pace of our work. At the same time, it's increasing the need for uniquely human capabilities. I often tell my team that tools can automate our procedures, but they can't yet replace judgment in ambiguous situations. That includes being adaptable when the risks and priorities shift quickly, strengthening our ability to influence key stakeholders, and helping shape decisions within our organizations.

There is little doubt that technology is evolving the profession and, more importantly, how our work is valued. Not long ago, internal audit's value was measured by the volume of testing we performed. Now it's defined by the risk insights we provide. From an internal audit perspective, that means showcasing our professional skepticism and ethical reasoning, effective communication, and ability to synthesize complexity into clarity.

Redefining Audit Work

Technology is not only changing what internal auditors do; it is fundamentally changing who they need to be. As digital tools scale, human interpretation and ethical oversight become the differentiators of audit quality.

Simply put, tools matter, frameworks matter, but when everything is moving faster and becoming more complex, it's still people — their judgment, confidence, and adaptability — that differentiate high-performing internal audit functions. That said, we should appreciate how technology is changing the day-to-day work of internal auditing and see how that fits into the broader discussion of the profession's value.

The IIA remains focused on equipping internal auditors to navigate this shift. By offering updated guidance, research, accessible tools, and professional development, we are strengthening both AI and technological fluency and the human capabilities that underpin effective auditing. I see this in three distinct areas.

Technology as an Enabler and a Disruptor. The growth of data-enabled assurance and analytics-driven audit work is making practitioners more efficient, and stakeholders recognize the potential for internal audit to do more with less. Meanwhile, technology risks dominate audit plans, particularly cybersecurity and IT. Yet technology adoption and maturity still lag expectations within many internal audit functions.

AI's Two-Tiered Challenge. AI is automating routine audit tasks, expanding analytical insight and predictive capabilities, and increasing expectations for speed, relevance, and clarity. At the same time, boards are turning to internal audit for assurance on AI governance, model risk management, transparency, and ethics. Failing to deliver on any of these tasks is unacceptable.

Technology and Human Capabilities. In the AI era, professional judgment, ethical reasoning, critical thinking, clear communication, and professional skepticism will be more valuable than ever. As automation scales,


Pulse Trends
Funding Sufficiency
30%
45%
25%
Mostly/ completely sufficient
Moderately sufficient
Not sufficient
Trend 2024-2025
53%
45%
30%
25%
25%
22%
Staff Level Change From Prior Year
11%
23%
59%
Increased
Stayed about the same
Decreased
Trend 2024-2025
64%
59%
25%
23%
18%
11%
SOURCE: THE IIA, 2026 NORTH AMERICAN PULSE OF INTERNAL AUDIT

Developing and empowering the next generation of practitioners is not optional; it is central to the profession's resilience, relevance, and existence. The future demands that internal auditors be fluent in technology and apply critical thinking and analytical judgment to complex, interconnected risks.

judgment does not diminish — it becomes more visible. AI raises the bar on speed and insight, but it also raises the bar on ethics, interpretation, and human discernment.

Building the Talent Pipeline

Talent is rising on the risk register. More than simply a human resources concern, it has become a risk management and resilience issue for internal audit functions. Gaps in skills, capabilities, or even culture can directly impact internal audit's ability to identify emerging risks and deliver timely, effective guidance. As such, each decision audit leaders make about whom we attract, how we develop them, and whether they remain in the profession is now a risk and resilience decision.

Developing and empowering the next generation of practitioners is not optional; it is central to the profession's resilience, relevance, and existence. The future demands that internal auditors be fluent in technology and apply critical thinking and analytical judgment to complex, interconnected risks. They must also excel at communicating insights in ways that influence organizational strategies. Yet the skills required to thrive in the AI era are evolving faster than traditional talent pathways can keep up.

Traditional career pathways assume that we bring someone in at an entry-level position, have him or her perform manual testing for a few years, and eventually develop into a senior role. But automation has eroded much of that early career work, increasing the skills needed for entry-level positions.

What I'm looking for today from new entrants to internal audit focuses on four key areas: digital fluency, critical thinking, business acumen, and effective communication. This mix of talents encourages more flexible career pathways.

I recently hired an internal audit manager. Because I knew AI was handling so much of the traditional testing, I needed someone with knowledge of the business, which is something AI doesn't have. AI can't put things into context or understand how things are really done within a business.

I ended up hiring a 20-year-career person from our operations team who is digitally fluent and has strong analytical thinking skills. This person can go through what AI is generating for us and say, "Does this seem right? Is it fit for purpose for us?" This matters because what I'm assessed on are the recommendations we provide the business. Are they practical? Are they reasonable? And ultimately, do they add value to the business?

Enabling Internal Audit's Future

Through student outreach, emerging leader programs, and credentialing, The IIA is directly addressing workforce constraints. It is equipping the profession with the standards, research, and developmental pathways needed to meet rising expectations. By investing in people at every stage of their careers, we strengthen trust, credibility, and long-term impact.

For example, the Internal Auditing Competency Framework aligns with the Global Internal Audit Standards and provides a structured model for auditors to develop skills in technology, leadership, professional judgment, governance, and risk insight. It gives internal audit functions a measurable roadmap to build staff capabilities. However, that must be paired with intentional leadership focused on upholding and adopting that framework.

By investing in research and guidance, The IIA helps internal auditors interpret the rapidly evolving risk environment and technology's impact. It also helps accelerate the transition from a compliance-focused function to a more strategic, insight-driven role that delivers forward-looking value to the organization. Practitioners must transform now or become irrelevant. For example, as technology replaces early-career tasks, such as note-taking during audit client meetings, young internal auditors need to look their stakeholders in the eyes and better understand the organizational context and the business.

Strengthening the talent pipeline will require focused initiatives on three key fronts: student outreach and academic partnerships, emerging leader programs, and global certifications such as the Certified Internal Auditor. These initiatives address widespread talent shortages identified by CAEs.

The Human Advantage

Internal auditors must recognize the pressure our stakeholders face to embrace AI and not be left behind in the digital marketplace. But we also should be cognizant of their growing awareness of AI's limitations and the need for human oversight of what AI produces.

While our stakeholders have readily embraced AI, they are going to be increasingly skeptical of its output once they start seeing too much AI-generated information that lacks relevance, applicability, practicality, and reasonableness. By recognizing, investing in, and developing skills that set humans apart from AI, internal audit can be the bridge that provides clarity and context.

David Helberg, CIA, CRMA, is chief, Internal Audit Services & Corporate Ethics and privacy officer at Cameco Corp. in Saskatoon, Saskatchewan.

AI TRUTH DECAY

Internal auditors need to radically expand their professional skepticism to assess the veracity of AI-generated information.

Joshua Goldsmith and Gabby Beaver

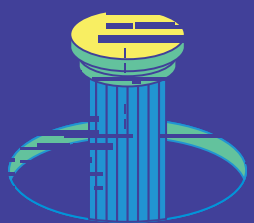
Although generative artificial intelligence (GenAI) can make operations more efficient, it also presents new challenges for internal audit. These concerns extend beyond the typical technology risks and into the fundamental nature of truth and evidence. Put bluntly, as AI becomes more integrated into business processes, it's becoming increasingly difficult to tell what is true.

In the February issue of *MIT Technology Review*, author James O'Donnell notes that even if readers know that content is generated with AI, it still shapes their belief in its veracity. In "What We've Been Getting Wrong About AI's Truth Crisis," O'Donnell cites a recent University of Bristol study published in the journal *Communications Psychology* in which participants watched a fake confession to a crime. Even after being told it was a deepfake, participants still relied on it when judging the individual's guilt.

The study's finding underscores the real danger posed by AI-generated artifacts.

TRUTH DECAY:

The diminishing role of facts and data in public and organizational discourse, driven by cognitive bias, information overload, and the increasing volume of opinion-based or misleading content.



This "truth decay" takes two primary forms:

- Malicious use of deepfakes to create fabricated evidence.
- Distorted narratives in documentation generated by GenAI.

For internal auditors, this new reality makes traditional evidence-gathering and review processes dangerously inadequate. They can't take the authenticity of video, audio, and even written documentation for granted. Auditors will need to rely on their professional skepticism more than ever.

Evidence in Doubt

The concept of truth decay has been studied extensively. RAND Corporation defines *truth decay* as the diminishing role of facts and data in public and organizational discourse, driven by cognitive bias, information overload, and the increasing volume of opinion-based or misleading content.

GenAI materially accelerates these dynamics by lowering the cost of producing content that appears authoritative despite lacking strong factual grounding, write RAND's Todd Helmus and Bilva Chandra in a 2024 article, "Generative Artificial Intelligence Threats to Information Integrity and Potential Policy Responses."

One example of this is deepfakes, which use GenAI to create hyper-realistic but fabricated images, video, and audio content. In 2024, a multinational firm in Hong Kong lost $25 million when a finance worker made a transaction after being deceived by a video conference populated with deepfake versions of senior executives, according to news reports. Similarly, AI can be used to alter audio recordings of customer complaints or video footage of inventory counts to conceal fraud or operational failures.

On the other hand, the existence of deepfakes could allow nefarious actors to deny the authenticity of genuine evidence, dismissing it as a fabrication. This once reliable form of evidence is now highly suspect.

False Confidence

Looking beyond malicious activity, there is a more subtle challenge to truth. When internal auditors use GenAI to draft reports, write post-postmortems, or create management summaries, they often unknowingly introduce a layer of "positive spin."

AI-generated employee self-assessments are an example. An outside reader of these assessments may conclude that the employee runs the whole company. Another example is using AI to write process descriptions, which can create distortions between what the description says is supposed to happen and what actually occurs.

In an online lesson, Andre Kutuzov, associate professor of natural language processing at the University of Oslo, notes that modern large language models (LLMs) have an overly positive bias. Researchers have found such bias when LLMs have been used for academic peer reviews and have noted that Google's NotebookLM has created positive reviews for scientific papers that had received "extremely low" ratings from human reviewers.

The models "tend to focus on strong or impressive aspects of the text under analysis, while ignoring downsides," Kutuzov writes.

GenAI models that are trained on a vast array of datasets are typically optimized to produce confident and polished narratives, Kutuzov explains. That makes the models helpful, harmless, and honest, but not critical where needed. This can lead them to embellish successes and frame neutral outcomes in an overly positive light.

As a result, AI-generated reports may minimize negatives and downplay failure or control deficiencies. It may also bury negatives in jargon or omit them entirely. Moreover, AI hallucinations can distort the truth by generating plausible but factually incorrect details to fill gaps in the model's knowledge.

For internal auditors looking to understand the true state of a process or the control environment, this AI-generated output is a significant obstacle. Although the documentation may appear comprehensive and well written, it can obscure the underlying reality of risks and deficiencies. That impacts the auditor's ability to identify red flags and areas requiring deeper investigation.

Intelligent Skepticism

To combat the challenge of truth decay, internal auditors need to sharpen their professional skepticism. A cornerstone of auditing, professional skepticism must be radically intensified and redirected in the AI age. Auditors must cultivate a mindset informed by technological understanding to form intelligent skepticism.

Intelligent skepticism involves questioning the source of the data and not just the statement. In theory, this would include understanding what model was used to generate the statement, how it was trained, and what parameters or context influenced the output. However, this information typically is not available. Major enterprise and consumer AI tools do not disclose detailed model architectures, training data sources, or real-time version changes.

This lack of detailed specifications is a limitation that professional skepticism alone cannot overcome. Auditors can't look inside the black box, nor can they independently validate the internal logic of these systems. This limitation reinforces the need to redirect assurance efforts away from AI-generated narratives and toward the integrity of the underlying data that feeds these systems.

Focus on Data

To be skeptical, it's no longer sufficient for internal auditors to review the final output such as a financial report, system log, or an executive summary. Auditors must look behind the curtain, beginning by verifying the raw data that feeds AI systems and the logic that produces them.

That means monitoring the integrity of critical data elements (CDEs) such as customer transaction amounts, validated employee IDs, and product pricing data. These are the essential data points supporting the organization's business functions and reporting. To validate CDEs, auditors should take several steps.

Identify CDEs. Auditors should begin by working with business units to determine the most important CDEs across key processes. They should document data definitions, authorized sources of record, ownership, access, and acceptable data quality tolerances.

Assess Governance. Internal audit should evaluate the design and operating effectiveness of controls governing CDEs, including data input validation, change management, access rights, reconciliation processes, and exception handling. Auditors should determine whether AI systems consume data directly from trusted sources or from downstream, transformed datasets.

Uncover the Foundational Data. Auditors should verify data lineage by tracking CDEs from their point of origin to their final use in reports, dashboards, or AI-generated outputs. They should check that CDEs have not been tampered with nor inappropriately transformed. The integrity of this foundational data is far more valuable and reliable as audit evidence than any AI-generated summary or report layered on top of it.

Test CDEs. Internal auditors should use data analytics or re-perform process steps, such as CDE generation or transformation, to independently test samples or full populations of CDEs to confirm the data is complete, accurate, valid, reliable, sufficient, and timely. They should treat AI-generated summaries or narratives as secondary artifacts that are useful for context but not as audit evidence.

Smarter Analytics

While GenAI introduces new risks to the integrity of audit

Auditors must be able to challenge AI systems, understand their limitations and biases, and question how their outputs are produced.

evidence, it also can support a more data-focused audit when used carefully and with appropriate controls. AI-powered analytics can help auditors identify and track CDEs by scanning documents, data models, and system metadata. In addition, these tools can monitor CDEs for anomalies, unusual patterns, or data quality issues in near real time. That can enable practitioners to focus tests on the highest-risk areas.

AI also can quickly map how data moves upstream and downstream across systems. It can flag undocumented changes or unexpected dependencies along the way.

While it should not be a primary source of evidence, AI can augment internal audits by improving coverage, timeliness, and precision. This gives auditors more time to apply their professional judgment, question assumptions, and base conclusions on verified source data, rather than polished narratives.

Reclaiming the Facts

With AI-generated data, internal auditors need to recognize that source data matters more than the narratives written about it. By prioritizing audits of data governance, lineage, and security, audit functions can build a more resilient and reliable assurance model.

Amid this shift, internal auditors need training on AI risks. Auditors must be able to challenge AI systems, understand their limitations and biases, and question how their outputs are produced.

Internal audit also should update its methods to require practitioners to validate source data for key reports and analyses, especially if auditors suspect this information was generated by AI. Investing in data analytics tools and skills can help internal audit independently test and verify the integrity of CDEs.

In addition, internal audit can partner with technology and data governance teams to learn how the organization is using AI and what controls are in place. To strengthen the organization's defenses, internal audit should use its influence to promote stronger data governance and CDE management, building on the structures already in place. By sharpening professional skepticism, focusing on data sources, and protecting the integrity of critical data, internal audit can help the organization meet the challenges of the AI era.

Joshua Goldsmith, CFE, CAMS, is head of Internal Audit Digital Solutions and Innovation at Citigroup based in New York.

Gabby Beaver is chief auditor—Technology & Business Enablement and Artificial Intelligence at Citigroup based in London.

SECRETS OF TOP AUDIT TEAMS

Recipients of The IIA's highest quality rating share what makes their audit functions effective.

Kim Kavin

It's breathing rarefied air to be among the internal audit functions that earn a "fully achieves" rating in an external quality assessment. IIA Quality Services results since the Global Internal Audit Standards took effect in January 2025 highlight that this outcome reflects an exceptionally high level of conformance and maturity (see "IIA Global Quality Certification" on page 42). "It recognizes a great achievement," says Warren Hersh, director of IIA Quality Services, "but it is absolutely within reach for all departments."

The good news is that when it comes to the best-of-the-best internal audit functions, there are commonalities in how excellence is achieved. It doesn't matter how big or small a

department is or what industry it's focused on. With significant preparation, supportive leadership, constant communication, technology aptitude, and the right staff, a "fully achieves" designation is possible.

Significant Preparation

A lot of thought goes into how to constantly improve the internal audit function at UMB, a financial services company based in Kansas City, Mo. CAE Bradley Kastler and Professional Practices Director Kristen Miller say they spent two years preparing for their recent five-year external quality assessment, with a specific focus on getting the team up to speed on all the Standards.

"We did a lot of department training when the Standards first came out," Miller says. "We did a lot of trial-and-error pilots."

The team incorporated a gap assessment defining paths forward, while also focusing on other requirements, including those of the U.S. Department of Treasury's Office of the Comptroller of the Currency (OCC), Kastler adds. "We have multiple standards for internal audit functions in our industry, and doing those gap assessments help as well," he says. "They ensure we're not only meeting the concepts, but also our Federal Reserve standards and our OCC expectations."

Leading performers undertake significant effort to fully conform with the Standards, says Susan Verghese, an IIA internal audit quality assessment reviewer. She notes that internal audit functions typically take six to 18 months to address the identified gaps after an assessment.

"It's not something that happens overnight," she says. "It's the mindset of the head of top internal audit functions. They want to be the best, so they want everything fixed — a good thing."

To stay relevant, internal audit must adapt, says Ruby Opara Collings, vice president, Global Internal Audit, at medical technology company Haemonetics in Boston. "We always think about a way to make the process or the system work for us more efficiently, and to be flexible and scalable," she explains. "We're constantly tweaking."

Supportive Leadership

Having C-suite buy-in is another key to success. Richard Lane, team leader for IIA Quality Services, says a good relationship with management is the biggest differentiator he sees with top audit functions. There needs to be an actual relationship with the client.

"What do they need from you? How can you help them be more successful?" Lane asks. "If you can

TOP SECRET

"We did a lot of department training when the Standards first came out. We did a lot of trial-and-error pilots."

Kristen Miller, Professional Practices Director, UMB

"We have multiple standards for internal audit... Doing those gap assessments helps as well."

Bradley Kastler, CAE, UMB

help them be more successful, they will welcome you. They're not going to see us as the enemy."

Anna Davis, vice president of internal audit and CAE at San Diego-based technology company Qualcomm, says having that kind of relationship helps her team thrive. "We have a solid line to the audit committee of the board of directors, and we have to be independent and objective," Davis says.

Although she reports to the company's chief financial officer, she is directly accountable to the audit committee. "The committee isn't involved in our day-to-day oversight, so it's really important to them, knowing that they have a fiduciary responsibility to shareholders to make sure the company's internal control environment is operating effectively," she explains.

Verghese, too, says success among top performers often starts at the top. "It's the tone that the CEO is setting for the organization, and the tone of the CAE who says, 'We're here to help you find issues before they hit *The Wall Street Journal* or have your external auditor or regulator tell you that you have a real issue.'"

Board support for internal audit is also key, Verghese notes. "How knowledgeable are the board members about internal audit and risk?" she asks. "In some organizations, they are very hands-off. In other cases, they are actively involved in making sure the organization's risks are being appropriately managed."

Verghese adds that having the right kind of people on an audit committee makes a real difference. Knowing what you're seeing in terms of improvements or omissions goes a long way. "You have to have people who understand risk, who can understand what it means if some things are happening in terms of achieving objectives," Verghese says.

The good news is nowadays that kind of competency exists in lots of places. "The strength and the capability of the audit committee really helps the internal audit function succeed, by supporting audit and ensuring our focus and resources are directed toward the company's strategic priorities, highest risks, and what matters most," she says.

Constant Communication

Communication matters in multiple ways. It includes talking within the internal audit team. "Whenever new people join the team, I do a one-hour orientation," Davis explains. "I want them to understand the expectations of our department in terms of the reputation and credibility that we have within the organization."

TOP SECRET

"We always think about a way to make the process or the system work for us more efficiently, and to be flexible and scalable. We're constantly tweaking."

Ruby Opara Collings, Vice President, Global Internal Audit, Haemonetics

IIA GLOBAL QUALITY CERTIFICATION

The IIA's updated Standards shifted focus from conformance with Standards to conformance plus performance. Under the previous Standards, conformance meant having appropriate documentation, policies, procedures, and the like. Adding performance to conformance also means demonstrating excellence through internal quality assessments, reporting results to audit committees, and putting in place action plans for improvement, Hersh explains.

Under the new Standards, there's a four-level rating scale for external quality assessments:

- Does not achieve
- Partially achieves
- Generally achieves
- Fully achieves

The "fully achieves" rating recognizes exceptional departments.

"There are things that departments are doing now to prepare themselves for the 'fully achieves' rating," Hersh says. Conducting a gap/readiness assessment is an effective way to identify areas for improvement and create a clear roadmap for conformance, which then helps internal audit prepare for an external quality assessment. "With this approach, they increase the likelihood of achieving that 'fully achieves' rating," Hersh adds.

Communication can help foster credibility, while a single misstep can destroy it. "Your credibility is damaged for quite a while until you can recover," she says. "We strive to be a trusted business partner, and we have to nail it on quality."

Building that kind of rapport requires communicating well beyond the times when audits are taking place, Lane says. "There are some people who only talk to their clients when they do audits," Lane explains.

That can be seen by clients as an adversarial situation if they are concerned auditors will discover something business unit leaders don't know about. "If you talk to people outside that time, you can build a good relationship," he says. "Then when you come in, they're not so nervous about what's happening in their department."

To prepare clients, Davis says her team gives an internal audit awareness presentation twice a year. It's a way to communicate the purpose of what's happening. "A lot of people may have never been audited before, and automatically, the perception is negative," she says. "So, we started doing audit awareness. We invite anyone we think we're going to audit in the next year. We tell them what to expect, and we're very transparent about what we're doing."

Technology Aptitude

Two types of technologies are making a difference for top-performing audit functions: data analysis and artificial intelligence (AI).

Verghese says today's tech can provide continuous feedback to stakeholders. It allows management to upload evidence online showing they have implemented the changes they

EXPERT TIPS

"There are things that departments are doing now to prepare themselves for the 'fully achieves' rating."

Warren Hersh, Director, IIA Quality Services

"There are some people who only talk to their clients when they do audits... If you talk to people outside that time, you can build a good relationship."

Richard Lane, Team Leader, IIA Quality Services

"Just having access to [technology] and using it to build relationships... differentiates some of the top-end organizations."

Susan Verghese, Assessment Reviewer, IIA Quality Services

promised. In turn, a CEO can go into the same system's dashboard and see how many management action plans are overdue — because an overdue action plan means the organization is still exposed to risks.

"Just having access to that kind of technology and using it to build relationships, that's a great thing," Verghese says. "It differentiates some of the top-end organizations."

Lane says data analytics can be used to spot trends and aberrations. "If something is an aberration, that means it's not controlled," he says. That lack of control indicating a possible risk the auditor needs to identify. "What's the problem you need to go look for there?"

One of Lane's clients recently spent a year and a half using AI to scan all the electronic information in the company, including manuals, legal requirements, and relevant public and internal documents. "Audit was using AI to go through all this documentation, to understand what the controls were, what the risks were, what the business was trying to accomplish," he explains. "From that information, they also developed their audit program."

The department also began using AI to write audit reports after training it on 6,000 previous audit findings. "Now they were moving into scanning all the electronic information provided by the company to help identify threats and weaknesses in the audit programs," Lane adds.

Davis says her team uses Microsoft Copilot to supplement their work. The team uses a report-writer agent that takes notes from auditors' work and drafts a report at the end of an engagement. It can create meeting notes and flowcharts of processes auditors are reviewing. "We also have a cybersecurity agent that can reference information on the internet, like professional standards and best practices," she says. "We can run the agent to review work we've done and point out anything we've left out."

The Right Staff

Kastler says having the right people within internal audit functions is paramount. Not only do they need to do the work and communicate effectively, but they also need to ensure that goals are being achieved within the audit framework.

"Our team is fantastic, and the quality assurance team and the talent there — it wasn't an afterthought," he notes. "Personnel really matters here."

Opara Collings says it's also important to continually elevate the staff's skills and create real career paths for individuals to grow. "We want to be true dynamic professionals," she says.

Kim Kavin is a freelance writer in Morris County, N.J.

TOP SECRET

"A lot of people may have never been audited before, and automatically, the perception is negative. So, we started doing audit awareness."

Anna Davis, Vice President of Internal Audit and CAE, Qualcomm


THE CHALLE

NGER SALES APPROACH

Adopting sales techniques can help internal audit shift mindsets and convince stakeholders to act on strategic advice.

Maxim Terlovsky Joshua Clark

Internal auditors are not expected to sell their services; the need for their work is cemented in organizational policies. Yet, in today's business environment, using sales techniques can be essential for facilitating auditors' day-to-day work and helping position internal audit for future challenges.

The IIA's Internal Audit: Vision 2035 findings highlight how internal auditors are expected to "enhance their role as independent, objective strategic advisors who provide tremendous value to their organizations." To earn the role of strategic advisor to the business, internal auditors must be able to share their unique insights across the organization and demonstrate to stakeholders the value of advisory services.

Auditors can use techniques developed by sales professionals to explain the value of their products and services to shift management's mindset. Sales techniques such as "reframing" — offering new perspectives on a known problem — can be useful in traditional audit engagement settings to help management understand audit findings and convince leaders to invest time and resources to remediate them.

Sales professionals have long focused on how to achieve the best outcome from a sales call — a crucial interaction with a customer. While techniques vary, they all focus on understanding customer psychology

and motivation, establishing trust, maintaining clear lines of communication, and uncovering problems the sales organization can help address.

A SALES-BASED FRAMEWORK

One sales approach that could benefit auditors is based on research from the 2011 book, *The Challenger Sale*. Authors Matthew Dixon and Brent Adamson upended the assumption that success in complex business-to-business sales was based on building amicable personal relationships. Their research identified five distinct profiles of sales representatives (see "The Five Profiles" on page 47). They found that in complex sales scenarios — which are similar to high-stakes, multi-stakeholder audit engagements — the "challenger profile" consistently outperformed all others.

A challenger's success is built on three core skills:

- ***Teach.*** Having a deep understanding of a customer's business allows internal audit to offer valuable insights that management hasn't previously considered. Challengers don't just talk about their product; they provide customers with a unique perspective on significant business problems they may be unaware of.
- ***Tailor.*** The challenger adapts his or her message to align with each stakeholder's specific problems, goals, and motivations. This ensures the message is relevant and resonates personally.
- ***Take Control.*** This means guiding the conversation assertively and confidently. Challengers are comfortable discussing sensitive topics and pressing for commitments, ensuring the process maintains momentum.

APPLYING THE MODEL

Auditors might wonder what valuable insights they can offer to stakeholders. No matter how knowledgeable auditors are in any subject area, they remain generalists by the very design of their profession. At the same time, line managers have years or even decades of experience in their fields, which are often narrow and specific.

Every line manager wears two hats. Each is responsible for the product. Managers are also responsible for the production process. While senior management's expertise usually lies in producing a high-quality product, their understanding of inherent risks and appropriate controls to address them may vary.

Internal auditors are positioned to provide a holistic view and connect the dots within a large, often siloed organization. They are experts at identifying process risks and evaluating well-designed control frameworks that support robust processes.

Auditors can educate stakeholders about risks they may not fully grasp or have even considered. In addition, auditors often have visibility into how processes connect across an organization, giving them insights into risks and challenges that fall outside management's immediate awareness or control.

This is where reframing becomes a powerful tool. An auditor can connect a seemingly isolated control deficiency to a larger, more significant business risk, such as regulatory risk, operational inefficiency, or strategic failure. This transforms the conversation from a technical fix of a particular segment of the management process to a strategic imperative. Internal audit's goal is to shift stakeholders from passively accepting — or actively resisting — audit findings, toward proactively addressing the real threats facing their processes.

The challenger model introduces a six-step "commercial teaching" approach, which can be translated for internal audit.

The Warmer. Auditors begin by demonstrating a deep, credible understanding of the stakeholders' business. They build rapport through a shared knowledge base, awareness of recent industry and regulatory events, and an understanding of internal and external risks and opportunities.

The Reframe. By connecting a familiar issue to a larger, more painful risk that stakeholders may not have recognized, the auditor presents a new perspective on a known problem. This insight can come from recent audit engagements or from auditors' awareness of new regulatory publications.

Another potential source of audit insights is "reading across," an analysis of issues identified within the organization and their potential impact on an area of management's interest. The issues may directly impact the stakeholders' process — for example, if data quality issues have been uncovered in a department that supplies data for their analysis and reporting. The issues may also have been identified in similar processes, prompting the auditor to raise the same concerns with the stakeholders' department.

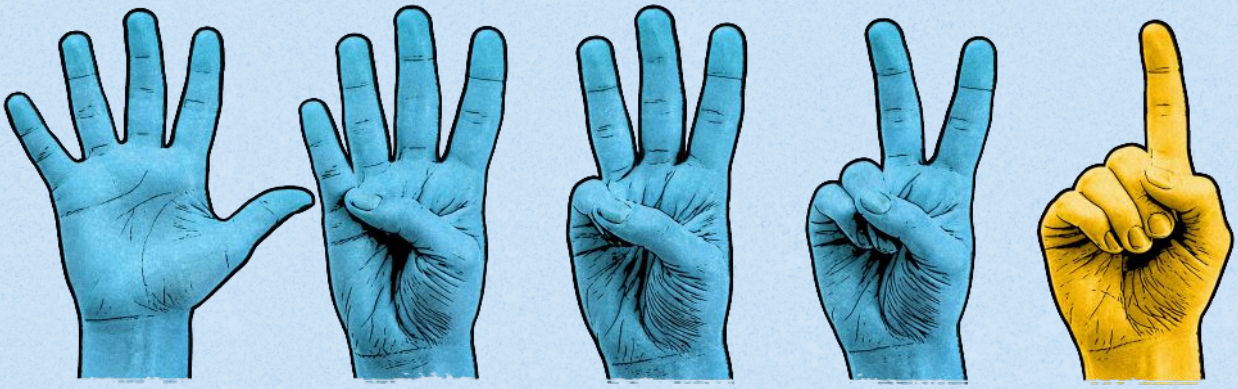
Rational Drowning. Using data, facts, and figures, the auditor presents a quantitative business case for change. In a world of limited resources and an ever-expanding array of conflicting priorities, management will always be focused on actions with the greatest material impact. Therefore, auditors should do their homework and present facts

to bolster their case for remedying the issue, demonstrating the seriousness of their concerns.

Emotional Impact. The auditor tells a story or uses a case study that resonates with the stakeholder personally, showing how a similar scenario could affect their team. Sales literature often suggests using emotional levers to prompt customer response. However, providing examples of consequences of inaction — such as a regulatory finding in another department, a fine levied on a peer company, or a negative article published in an industry publication — may motivate more reactive managers to act.

A New Way/Your Solution. At this stage, a salesperson would introduce his or her product as the perfect solution to a newly identified problem. The auditor's role, however, is to prompt a discussion about a new way forward without providing the solution, itself. While auditors may have a preference based on their own industry experience or insight into peer processes, it is important to rely on stakeholders' expertise and empower

THE FIVE PROFILES



1. THE HARD WORKER

They show up early, stay late, and always go the extra mile. They are self-motivated, persistent, and open to feedback and personal development. They believe doing the right things (making more calls, sending more emails, doing more research) will lead to success.

2. THE RELATIONSHIP BUILDER

This profile focuses on building strong relationships. They are generous with their time, highly accessible to customers, and strive to alleviate tensions and resolve conflicts. They believe if the customer likes them and trusts them, business will follow.

3. THE LONE WOLF

The Lone Wolf is self-confident, intuitive, and naturally rule-breaking. They do things their own way, ignoring processes, customer relationship management requirements, and management directives. They are difficult to manage, but leaders tolerate them because they consistently deliver strong sales results.

4. THE REACTIVE PROBLEM SOLVER

These reps are detail-oriented and reliable. To customers, they are valuable because they immediately jump in to fix any post-sale issues, ensuring implementation goes smoothly. However, they tend to focus more on solving current problems than on generating new demand or pushing the sale forward.

5. THE CHALLENGER

The Challenger operates with a deep understanding of the customer's business and uses that knowledge to push the customer's thinking and teach them something new about their company to help them compete more effectively. They are not afraid to share controversial views, they are assertive about pricing, and they actively take control of the sales conversation rather than just responding to the customer's requests.

CHALLENGING STAKEHOLDERS' ASSUMPTIONS WILL INEVITABLY CREATE TENSION. AUDITORS SHOULD LEARN TO STAND THEIR GROUND WHILE TURNING UNPRODUCTIVE CONFLICT INTO "CONSTRUCTIVE TENSION."

them to own the solution and remediation.

TAILORING THE MESSAGE

To be effective, auditors must tailor their communication to their audience. Different positions within an organization require different insights to ensure buy-in.

When presenting to senior management and the board, internal audit should focus on high-level, strategic findings, business impacts, and actionable recommendations. Discussions with line management should include more focused insights, detailed data-driven evidence, and practical, process-level recommendations.

In addition, internal audit must take control of the narrative to guide the path to remediation. This means using a clear, direct, and assertive communication style.

This involves ensuring that management's action plans are detailed, include clear expected outcomes and success metrics, have clear ownership, and include aggressive but realistic deadlines. A valid finding alone, without decisive corrective actions, may not fully address the risk. Finally, auditors must ensure management's actions have been completed and validate the remediation of the issue.

BECOMING A CHALLENGER

While organizations invest time and resources in training their sales force, an auditor's interpersonal skills training usually does not go beyond basic communication skills. Internal audit should place as much emphasis on communication and influencing techniques as it does on technical knowledge, especially for auditors who interact with senior stakeholders.

In addition to communication techniques, the training should also address business acumen and resilience. Challenging stakeholders' assumptions will inevitably create tension. Auditors should learn to stand their ground while turning unproductive conflict into "constructive tension," creating a high-impact engagement.

The challenger model emphasizes learning to reframe risks, tailoring the message, and creating constructive tension so auditors can change the outcome of a high-stakes engagement. At a time when internal audit must act with a more commercial mindset, competing for management's focus and the company's scarce resources, the ability to make a compelling, risk-based case actually delivers results.

Maxim Terlovsky, FRM, is chief auditor of Markets at Citigroup in New York.

Finding Patterns in Public Disclosures

By using AI to study the clues in other organizations' risk factor disclosures, internal auditors can benchmark their own company's risks.

Walied Keshk and Jiwon Nam

Known risks can be monitored and mitigated, but unknown risks can blindside an audit function and its organization. That's why identifying risks that could materially affect an organization's business or securities is a crucial part of strengthening risk management and governance.

One valuable source for identifying risks is Item 1A–Risk Factor disclosures, which U.S. publicly traded companies are required to include in 10-K and 10-Q filings to the U.S. Securities and Exchange Commission (SEC). Since they were first required in 2005, Item 1A disclosures have provided investors and other stakeholders with information about the company's most significant risks.

Internal auditors can use their company's Item 1A disclosures — as well as those of competitors, suppliers, and customers — to better assess, prioritize, and address key risks such as cybersecurity, supply chain disruptions, and regulatory change. Even auditors at companies that are privately held or outside of the U.S. can benefit from analyzing Item 1A disclosures because many of the risks affect organizations across industries and regions.

Artificial intelligence (AI) tools such as ChatGPT can significantly reduce the effort and cost of processing lengthy Item 1A disclosures. Internal auditors can retrieve these disclosures, analyze them using ChatGPT, and evaluate the results to identify their own company's significant risks. In addition, they can compare their company's assessed risks to those of industry peers to detect gaps, reevaluate likelihood and impact, and allocate audit resources more effectively.

Aggregating Data

Auditors can retrieve 10-K and 10-Q filings from the SEC's Electronic Data Gathering, Analysis, and Retrieval (EDGAR) database and extract Item 1A disclosures. This process can be done manually for a few disclosures or using Python web-scraping tools for larger samples.

Risk factor disclosures are often lengthy. AI can help auditors review this data quickly to spot patterns in risk categories and specificity by counting reported risks and assessing whether the disclosure's sentiment is positive, negative, or neutral. This helps auditors pinpoint differences in risk reporting across companies.

Using AI tools to analyze Item 1A disclosures can help internal auditors:

- Categorize risk factors.
- Compare risks across companies in their industry and over time.
- Identify new and evolving risks and assess their likelihood and impact.
- Update controls and audit plans.
- Achieve greater efficiency and effectiveness of their work.

Smaller companies often lack resources for in-depth risk analysis, making peer comparisons especially useful. An analysis of Item 1A disclosures from 2021 filed by eight, small U.S.-based pharmaceutical companies provides insights for internal auditors (see "Pharma Companies Risk Disclosure Analysis" on page 51). The market capitalizations of these companies range from $232 million to $286 million.

Risk Categories. ChatGPT identifies main risk categories by scanning the disclosures, clustering concepts, and applying its knowledge of industry disclosure norms. This categorization provides internal auditors with a useful and practical way to think of their organization's risks and compare them to the risks of industry peers.

Sentiment. ChatGPT evaluates the tone or sentiment of a company's Item 1A disclosures by classifying financial accounting words and phrases as positive, negative,

or neutral. Internal auditors can compare their company's disclosure tone to that of industry peers to identify disclosures that are overly positive or negative. Cases of over-optimism, when peers' disclosures are negative, may indicate the company failed to identify significant risks or assess their likelihood or impact. In the pharmaceutical case study, all companies had a negative disclosure tone, except Company C, whose disclosure tone was neutral.

Specificity. Internal auditors should monitor the level of specificity of their organization's risk disclosures and compare it to that of industry peers. ChatGPT measures disclosure specificity by comparing the number of company-specific references — such as referring to the organization, its products, customers,

Pharma Companies Risk Disclosure Analysis

The Item 1A disclosures of eight small, U.S.-based pharmaceutical companies were uploaded into ChatGPT-4o and given anonymized labels. Researchers analyzed them using the prompt shown below.

This table summarizes ChatGPT's analyses of the eight pharmaceutical companies.

PROMPT

These files include Item 1A, risk factor disclosures, made by eight small U.S.-based pharmaceutical companies for 2021. Please analyze these disclosures and identify the main risk categories disclosed by the companies. Next, present a table that includes the following for each company:

- ***Keyword count** for each main category of risk identified.*
- ***Total word count** for each company disclosure.*
- *A rating of the **specificity** of each company disclosure using the following scale: Highly specific, somewhat specific, boilerplate heavy.*
- *A rating of the **tone** or sentiment of each disclosure using the following scale: Positive, neutral, negative.*

FIRM	TOTAL WORDS	SPECIFICITY	TONE	RISK CATEGORIES: DEVELOPMENT & CLINICAL TRIAL	FINANCIAL & CAPITAL NEEDS	COMMERCIALIZATION & MARKET ACCESS	COVID-19 & PANDEMIC	MANUFACTURING & SUPPLY CHAIN	INTELLECTUAL PROPERTY & LEGAL	CYBERSECURITY & DATA PRIVACY	MARKET & ECONOMIC CONDITIONS
A	35,535	Somewhat Specific	Negative	834	156	543	72	76	269	17	177
B	24,895	Boilerplate Heavy	Negative	639	90	332	16	28	338	6	87
C	13,170	Somewhat Specific	Neutral	304	80	221	34	28	161	6	56
D	37,521	Boilerplate Heavy	Negative	910	123	422	95	102	357	22	106
E	31,798	Highly Specific	Negative	681	116	511	51	57	349	12	72
F	38,376	Somewhat Specific	Negative	793	122	456	56	145	495	32	108
G	19,469	Boilerplate Heavy	Negative	463	96	239	46	82	142	19	71
H	8,981	Highly Specific	Negative	290	67	118	12	45	63	2	53

or partners — to the number of vague, standardized, or generic phrases, commonly known as boilerplate language.

A high-level of boilerplate language suggests that the company did not take reasonable time and effort to identify and report the risks that endanger its business and securities. This increases the likelihood that the organization may have missed significant risks or may not have assessed their likelihood and potential impact reasonably.

Of the eight companies in the case study sample, two disclosures are highly specific, three are somewhat specific, and three use boilerplate language heavily. This should be a red flag for the internal auditors of Companies B, D, and H, whose Item 1A disclosures are rated as boilerplate-heavy.

Total Word Count. The "Pharma Companies Risk Disclosure Analysis" table reports the total word count of each company's Item 1A disclosure. A very low word count, compared to that of industry peers, may suggest that the organization did not allocate adequate resources to identifying, assessing, and reporting its significant risks.

For example, Company H had the shortest Item 1A disclosure among the sample companies, with fewer than 9,000 words. Because Company H's disclosure is rated as boilerplate-heavy, this suggests the company may be omitting important risks.

Keyword Count. For each pharma company, the table also reports the keyword count for each of the eight main risk categories identified by ChatGPT. Internal auditors can benefit in several ways by analyzing their own organization's keyword counts and comparing them to those of industry peers.

A self-reflective keyword count can reveal which areas of risk are perceived to be the most important or challenging, according to management. Internal auditors can then align their audit plans and activities with management's perceptions.

Alternatively, internal auditors can compare their organization's keyword count with their own risk assessment to make sure management has a clear view of the company's most critical risks. Further, auditors can track keyword counts for their organization and its peers. This helps practitioners identify new or emerging risks sooner.

For example, the keyword counts for the eight pharma companies show that their most important risk categories are:

- Product development and clinical trial risks.
- Commercialization and market access risks.
- Intellectual property and legal risks.

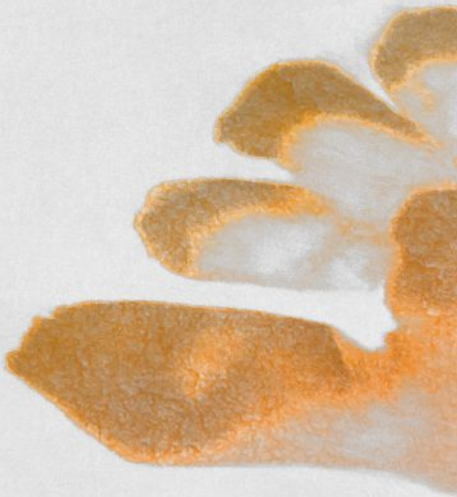
This is not surprising, given the fact that these are small, less mature companies focused on developing new pharmaceutical and biotech products. The analysis also reveals that Companies C and H have the lowest keyword counts, consistent with their shorter Item 1A disclosures. This may indicate they are overlooking risks or underestimating their likelihood and impact.

The pharma company disclosures only briefly discussed cybersecurity and data privacy risks, which had the lowest keyword counts. This is notable because these risks became more frequent and complex in 2021, as more companies moved to remote work during the COVID-19 pandemic. In these companies, internal auditors should determine whether their organizations truly face lower exposure to these risks or whether management underestimated them at the time.

The Path to Resilience

Internal auditors can use AI to analyze Item 1A disclosures in other informative ways. For instance, internal audit can compare Item 1A disclosures over time to identify changes, omissions, and inconsistencies, measure shifts in tone, and check alignment with SEC requirements.

Auditors can also find detailed risks within each main risk category that are disclosed by other companies in their industry sample. This analysis can help



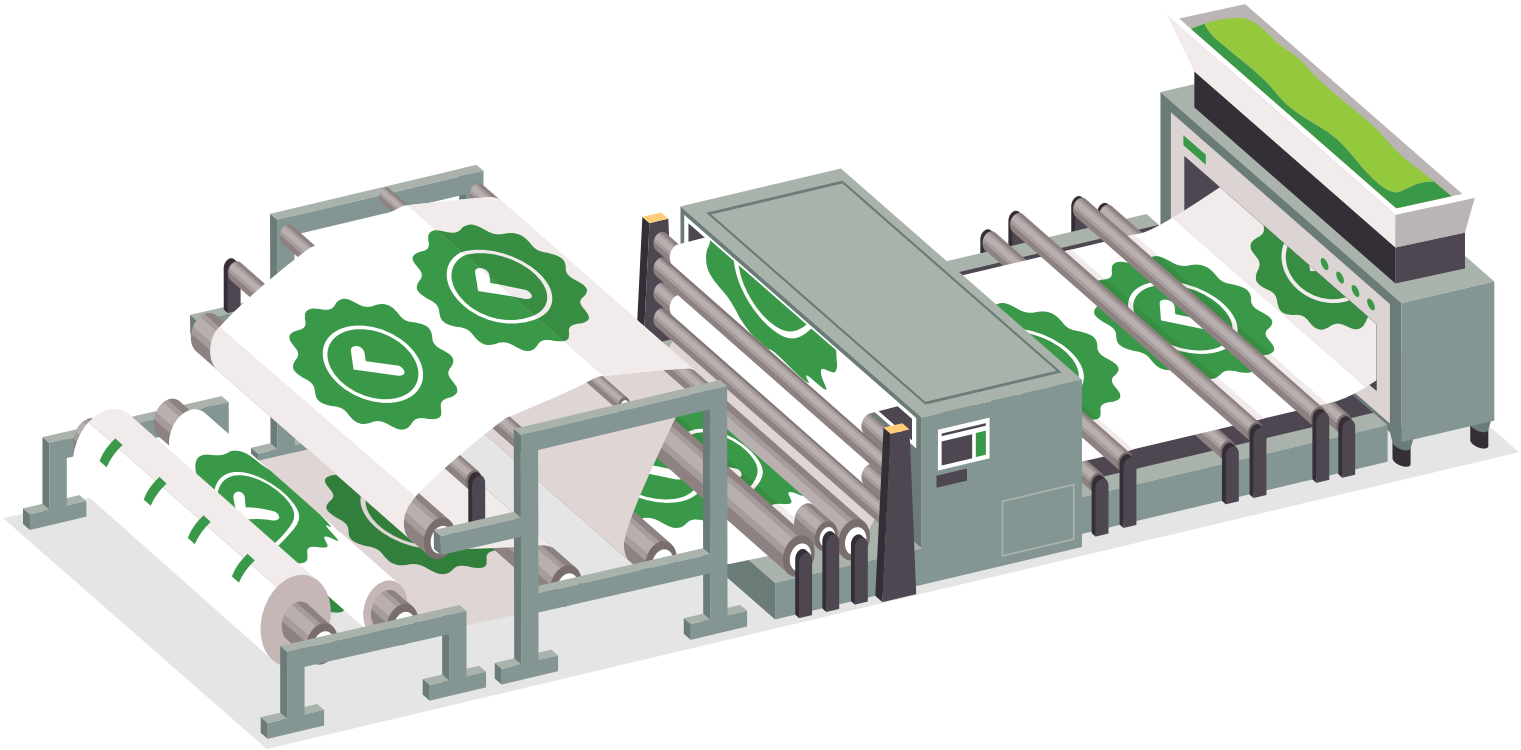
identify risks that may have been overlooked by their own company but are being discussed by peers.

Moreover, auditors can use disclosures to distinguish between organization-specific and industrywide risks, allowing for deeper, more accurate evaluations. Finally, auditors can examine whether their organization manipulates its Item 1A disclosures strategically, such as by using an overly positive disclosure tone amid poor performance, or using vague, complex language to obscure key risks.

Analyzing Item 1A disclosures can improve the quality of risk assessments, compliance checks, and audit planning. This process can motivate internal auditors to refine testing procedures, ensure appropriate controls are in place, and align audit priorities with disclosed risks. The ultimate outcome is stronger governance, reduced legal exposure, and enhanced long-term organizational resilience.

Walied Keshk, PHD, CPA, is an associate professor of Accounting at California State University Fullerton in Fullerton, Calif.

Jiwon Nam, PHD, is an assistant professor of Accounting at California State University Fullerton.



boardroom

Rubber-Stamp Audits

Boards must question the reliability of SOC audit mills offering cheap, easy assurance.

Matt Kelly

For the better part of a decade, the top risk on board directors' minds has been cybersecurity — especially the risk that a vendor's weak cybersecurity might harm their own organization. Though boards recognize the risk, one primary mechanism to manage that risk is coming under strain.

That mechanism? The system and organizational controls (SOC) audit, which technology and service providers can undergo to assess the effectiveness of their controls over financial reporting (a SOC 1 audit) or over privacy and cybersecurity (a SOC 2 audit). Ever since the American Institute of Certified Public Accountants (AICPA) established SOC audits 15 years ago, these audits have been a tool that organizations can use to help understand the security risks vendors pose to operations.

Lately, however, lots of noise has swirled up around "audit mills" as legions of software vendors promise SOC reports that are cheap, easy, and quick — which isn't how SOC audits are supposed to work. Corporate boards and risk assurance teams will need to pay attention to where SOC audits come from, and how much assurance those audits really provide.

"There is some stuff going on in the marketplace that is not great, and people need to understand the difference," says Amy Pawlicki, New York-based vice president of assurance and advisory innovation at the AICPA.

Delving Into the Details

The spark that ignited these concerns was an anonymous whistleblower who published allegations in March on Substack that a governance, risk, and compliance technology provider had fabricated results for nearly 500 SOC audits, which then were allegedly rubber-stamped by fake audit firms. That meant that any businesses relying on those audits wouldn't have a correct understanding of the security risks they face.

"There is some stuff going on in the marketplace that is not great, and people need to understand the difference."

Amy Pawlicki, Vice President of Assurance and Advisory Innovation, AICPA

Board directors should consider the larger issue here: Namely, that hordes of technology vendors are racing to provide SOC audit services, promising speedy work and low cost. If boards and audit teams don't pay attention to the details, they could end up with low quality assurance.

Let's pause here to remember how SOC audits are meant to work. First, someone needs to collect the evidence of a vendor's internal controls; then a CPA in good standing makes a formal assessment about whether those controls are designed properly (a Type I SOC audit) and that the controls work as intended over time (a Type II SOC audit).

Done correctly, SOC audits are nobody's idea of a fun time. The work can be painstaking, take several months to complete, and cost tens of thousands of dollars, at least. But in the end, anyone reviewing the SOC audit should be comfortable that the conclusions are reliable.

What's changed is the arrival of compliance tech vendors promising that they can automate the collection of that evidence. If that vendor is ethical and competent, great; it can pair up with an audit firm that reviews the

evidence and assesses the client's internal controls, done in less time and at less cost.

Unethical compliance tech vendors, however, can be a big problem. Some might engage in outright fraud, fabricating evidence and working with "auditors" who are little more than a mailing address. Others might churn through gathering evidence in a template-driven, one-size-fits-all format that doesn't capture the necessary insight and nuance.

"If a company has the maturity and experience to understand the intent of the SOC report, I'd like to think [SOC validity concerns are] relatively short-lived."

Martin Jung,
Vice President of Internal Audit and Risk Management, Premera Blue Cross

Vendors promising "SOC certification" rather than an audit is a red flag. The AICPA is trying to deliver that message via numerous articles and resources this year, all stressing the importance of SOC attestations and audits.

"We're shedding light on some practices going on in the marketplace that service organizations and the companies that rely on those organizations need to be aware of, so they're making good decisions," Pawlicki says.

Getting Better Assurance

The board should make sure management is taking the need for security assurance seriously. Exactly how depends on where in the SOC assurance world an organization sits.

For example, if an organization is a technology or service provider to corporate clients, the board should be sure management is not relying on some fly-by-night outfit promising a SOC certification. On the other hand, if an organization relies on service providers, management (typically the chief information security officer or vendor risk management team) should insist on SOC reports that are trustworthy.

"If a company has the maturity and experience to understand the intent of the SOC report, I'd like to think that concern is relatively short-lived," says Martin Jung, vice president of internal audit and risk management at Premera Blue Cross in Washington state.

In his position, Jung both receives and generates SOC reports. He isn't so much worried about larger, mature organizations skimping on security assurance. But smaller, younger startups, under pressure to grow quickly? "That's where I have the concern that the company might be interested in going to one of those other firms," he says.

That's where boards will need to keep management focused on what matters most; not what's cheapest and easiest.

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.

Action Items

For all the concern around SOC audits, they can be valuable sources of assurance that boards, management teams, and business partners want to see. So, when reviewing a SOC audit, boards should consider a few questions.

Was the audit scoped correctly? SOC audits can examine any (or all) of five "trust service criteria" defined by the AICPA. Not every SOC audit needs to include all five criteria, but a SOC audit that omits relevant criteria won't provide the needed assurance. Boards should pay close heed to who decided the scope of the audit and why they defined the scope as they did.

Is the auditor who performed the review credible? Beware of audit mills that might exist simply to rubber-stamp a preferred conclusion. The auditor should be a CPA from a firm without any disciplinary issues and have relevant experience.

Is the underlying evidence relevant and trustworthy? In a world where fly-by-night vendors promise audit evidence with low cost and fast results, the risk of shoddy work abounds. The board should consider where the evidence came from and whether it's reliable.

How important is high audit quality versus low audit cost? If boards want a quick SOC audit that checks a box but provides little assurance, they can easily find one. The real question is how much they are willing to pay for assurance over its vendors.

David Salierno

Employee languishing may be costing businesses more than they realize.

As engagement shifts, productivity, efficiency, and innovation can suffer in ways that aren't always visible.

Bare minimum Mondays, quiet vacationing, "resenteeism," soft off days. These aren't just cynical workplace buzzwords — they reflect real trends often overlooked by organizational leaders.

This is a widespread phenomenon. According to The Workplace Wellbeing Report 2026 from the Center for Professional Responsibility in Business and Society at the University of Illinois Urbana-Champaign, more than 60% of the nationally representative 2,000 U.S. employees surveyed are languishing, rather than flourishing, in their jobs.

The report describes *languishing* as a condition where workers struggle with engagement, motivation, or fulfillment. Oscar Ybarra, professor of business administration at the university's Gies College of Business, led the research and offers important distinctions about what languishing is — and isn't.

"It's not burnout, and it's not psychological distress or clinical depression," he explains. "The best way I can describe it is feeling like you're treading water at work. You're not miserable, but not super motivated — and you don't feel like you're growing or that you're part of something bigger that's meaningful."

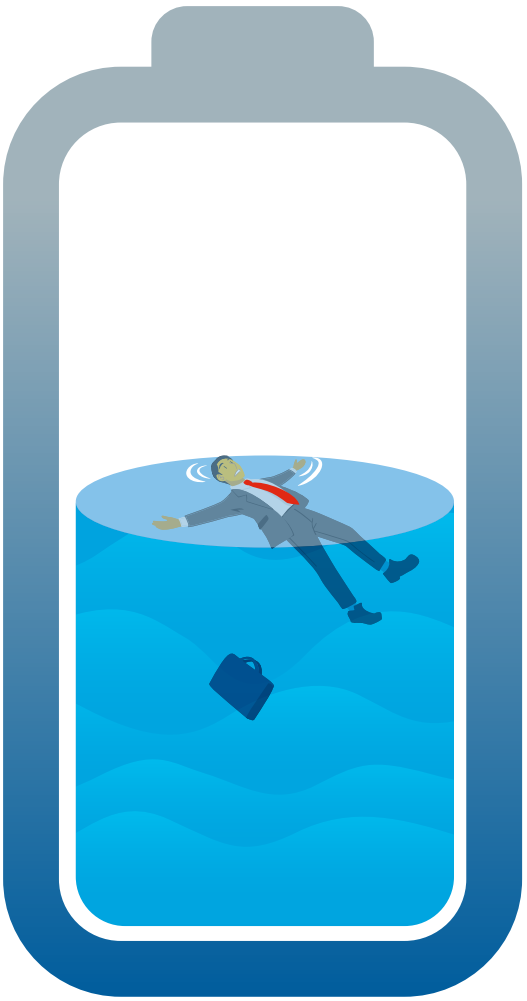
Over time, that languished state can take a significant toll on how people experience their work. It could lead to mental fatigue, stalled personal and career growth, a reduced sense of purpose, and an increased risk of burnout and depression.

But it's not just a mindset issue. Left unchecked, languishing can have significant business consequences. Understanding what drives languishing and how companies can address it may be crucial to harnessing employee potential and improving organizational outcomes.

A Silent Problem

Despite its prevalence, languishing can be difficult for leaders to recognize. "With severe anxiety or depression, symptoms can be pretty acute and noticeable," Ybarra explains. "But with languishing, employees feel like the conditions they need to perform well aren't there, and it's hard to put your thumb on it."

Because languishing doesn't always present as a clear crisis, it can persist unnoticed, evolving into more significant challenges.



The Workplace Wellbeing Report shows that, compared to employees who are flourishing, 38% of languishing employees say they "very frequently" feel burned out (versus 29% of flourishers). Additionally, about one-third say they plan to look for a new job within the next year.

These symptoms can spell trouble for the organization. Ybarra says the impact ranges from reduced engagement to increased turnover risk.

"When people experience languishing, they aren't able to focus deeply on their work," he says. "In terms of innovation, creativity, collaboration, and willingness to go above and beyond, there could be a real shortfall. Overall, you're just not getting the best out of people."

Even organizations with strong technology, financial resources, and market opportunity may struggle to perform at their full potential if key employees are languishing. Those strategic and tactical advantages are only as effective as the people executing them — and that becomes a lot harder when engagement is low.

Plus, when languishing becomes more widespread, the problem can compound, creating a corrosive climate. "Where people are sharing negative feelings and commiserating, the culture, itself, can degrade to some degree

and create a less engaged, less motivated environment overall," Ybarra says.

What's Driving This Trend?

Languishing isn't limited to a particular demographic. The Workplace Wellbeing Report shows it appears across age groups, income levels, genders, races, industries, and geographic regions within the U.S. It's also equally present across job roles.

That suggests the issue isn't tied to individual traits or specific types of work. Instead, the research points to workplace conditions as the underlying driver. In particular, it shows employees are less likely to flourish when they lack a foundation of autonomy, support, and trust. "Autonomy, the sense that there's direction and choice in your work and how you get it done — and support from the people around you — are important because they speak to fundamental human needs," Ybarra says.

Without a culture of trust, people doubt their own decisions or management's decisions — or the reliability of their co-workers. "You're not able to fully get immersed in your work," Ybarra adds, "because you have other concerns on your mind."

Can Languishing Be Overcome?

So, what separates workplaces where employees struggle from those where they thrive? According to Ybarra, it all comes down to what he describes as "work squads."

"It's a dynamic where you have work teams or groups that seem empowered, where employees feel they have some choice in how they do their work, some autonomy, some self-direction," he explains. "And they also feel like they have genuine support from their supervisors and from co-workers."

The difference can be significant. The report found that, within these empowered squads, nearly 70% of workers flourished. By contrast, only 10% flourished in environments that lacked these conditions.

Ybarra emphasizes, however, that it's not enough to meet employees' material needs. Creating an environment where employees can flourish requires organizations to address the psychological side of work in addition to pay, benefits, and incentives. "The psychological needs that employees have — to grow personally and professionally, to have some more responsibility, to feel like they're contributing — these are needs we all have," he explains. "And if you're not getting those, even if you're being paid well, it's going to lead to languishing."

Ybarra's research also highlights a strong connection between well-being and the organization's ethical environment. Employees are far more likely to thrive when expectations around ethics are well-defined and accountability is applied consistently. Under those conditions, people aren't drained by uncertainty or forced to navigate ambiguous situations or concerns about fairness. Instead, they can focus on their responsibilities, knowing that integrity is recognized and that the organization's actions align with its stated values.

90,000 Reasons to Care

The business case for employee well-being is clear, but the human one is just as important. It defines the day-to-day work experience in ways that go beyond metrics and results.

"We spend so much time at work — something like 90,000 hours across our career," Ybarra says. "I would rather have people have higher well-being, who are really engaged with the work they're doing for such a big part of their life."

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

> "In terms of innovation, creativity, collaboration, and willingness to go above and beyond, there could be a real shortfall. Overall, you're just not getting the best out of people."
>
> **Oscar Ybarra**, Professor of Business Administration, University of Illinois Urbana-Champaign, Gies College of Business

Following the Money

In the financial services industry, internal audit must adapt its oversight of changing regulatory, technological, and consumer demands.

Maria Mora, Partner, Crowe

Where are banks seeing gaps in controls?

Crowe's benchmarking data shows that compliance audits related to U.S. regulations around the Bank Secrecy Act (BSA), anti-money laundering (AML), and the Office of Foreign Assets Control (OFAC) produce the highest volume of significant findings — particularly around enhanced due diligence, customer risk ratings, OFAC screening, and transaction monitoring. Notably, many of these are not one-time issues. On average, internal audits are identifying approximately two recurring findings per audit, pointing to deeper structural challenges rather than isolated breakdowns.

Third-party risk management and IT general controls (ITGC) continue to surface as consistent pressure points, as well. Organizations are still struggling with due diligence, governance, and the ongoing monitoring of third parties. Among significant ITGC findings, 43% are tied to logical security weaknesses.

What's increasingly clear is that enterprise risk management is also emerging as a gap, not because controls don't exist, but because risks are not always being managed cohesively across functions. The common thread across all these areas is that the gaps are less about whether there is a control in place and more about how effectively those controls operate in complex, changing environments.

What are the root causes of these control gaps?

The root causes point to a disconnect between how controls are designed and how they operate in practice. While many findings are initially attributed to surface-level issues, such as training gaps or policies not being followed, these are often symptoms of the underlying problem.

More than 50% of significant findings are tied to missing, inadequate, or outdated policies and procedures, according to the Crowe 2025 Financial Services Internal Audit Benchmarking Study. At a broader level, that raises a more fundamental issue: whether control frameworks are reactive in nature, or truly resilient as risks grow and change.

Equally important is accountability. Our benchmarking data shows that issues such as unclear ownership and oversight failures were associated with at least one significant finding per audit, on average. When accountability is fragmented, even well-designed controls can fail.

We also see recurring challenges in process design and integration, particularly in operational areas such as BSA, third-party management, and IT. Many organizations address findings in isolation, without fully connecting them to broader governance or process issues. That's why repeat findings are so common, because the underlying drivers, not just the symptoms, remain unresolved.

How can internal audit improve oversight?

Internal audit can strengthen oversight by using benchmarking to evaluate whether the organization is auditing the right risks at the right depth. That starts with going deeper on root causes and challenging whether findings reflect isolated execution gaps or broader issues in governance, accountability, or process design.

It also requires a more integrated view of risk. Rather than assessing controls in silos, internal audit should evaluate how risks, particularly in areas such as BSA/AML, third-party oversight, and IT, are managed across functions, and whether programs are adapting as the business and regulatory environments shift.

Data and benchmarking can play an important role, but primarily as a way to inform perspective, not to replace judgment. The most effective internal audit functions use these insights to challenge assumptions, validate risk coverage, and bring an external lens to internal conversations.

Internal audit strengthens its value to management and the board when it can translate findings into clear insight on control effectiveness and risk exposure. When those discussions focus on why issues persist, not just where they occur, internal audit can help organizations move beyond remediation and toward more resilient, sustainable control environments.

More than 50% of significant findings are tied to missing, inadequate, or outdated policies and procedures, according to the Crowe 2025 Financial Services Internal Audit Benchmarking Study.

Tyler Graham,
Managing Director, CAE Solutions, Protiviti

What are the financial industry's macro risks?

Financial services firms are operating in a rare moment when regulatory clarity and innovation appetite are expanding at the same time. That convergence creates a significant opportunity — but also heightens operational and strategic risks for institutions that move too slowly in response to this rapidly evolving, competitive landscape.

One of the biggest risks is speed — both moving too fast and not moving fast enough. Technology, data, and product innovation are advancing faster than many traditional governance and control models were designed to support. At the same time, institutions are operating in increasingly complex systems that span multiple cloud providers, third party platforms, and digital assets. When something breaks, the impact is broader, more interconnected, and harder to predict.

Organizations that involve risk management and internal audit early — rather than retrofitting controls later — often move faster because they avoid last minute surprises. Trust is no longer just a compliance outcome; it's becoming a competitive advantage. The firms that will win are the ones that treat risk management as a strategic enabler, not a brake.

How are consumer expectations changing business?

People want financial services to be instant, simple, personalized, interoperable, and intuitive. Real time payments, seamless digital onboarding, and 24/7 access are no longer "nice-to-haves." They're expected.

The next wave of products will be seamlessly embedded into daily life across platforms. They'll also be transparent and aligned to a customer's social, moral, ethical, cultural, and economic beliefs and priorities. And they'll be increasingly programmable to adapt to customer needs and preferences.

To meet those expectations, large, end-to-end processes are being broken into modular services driven by application programming interfaces. Third-party use is expanding and becoming increasingly interconnected and integrated so products can evolve more quickly. Product teams are being held accountable, not just for launching features, but for managing risk across the entire customer experience. And control functions are moving away from periodic reviews toward continuous, data-enabled monitoring.

This shift also changes the role of internal audit and risk. The teams that add the most value today understand the customer journey across ecosystems, not just internal process maps. When auditors can see how controls, data, and decisions affect real customers in real time, their insights become much more relevant to the business.

What are the opportunities amid disruption?

Changes in the financial industry are forcing companies to rethink what makes them valuable and relevant. We are seeing traditional institutions adopt fintech-like speed and experimentation, while fintechs are providing traditional services and adopting bank-grade governance.

The shifts in the regulatory environment have made the competitive playing field more level, and institutions have an opportunity to stand out through product design, transparency, and customer experience — rather than simply relying on the advantages they've had for being around longer. This shift ultimately benefits consumers through better, more responsive financial solutions.

The future belongs to organizations that align business strategy, technology, risk management, and audit execution from the start — because in today's financial services environment, experience, credibility, and resiliency have become the strategy.

Changes in the financial industry are forcing companies to rethink what makes them valuable and relevant.

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

IPPF

What's New

TOPICAL REQUIREMENT

Organizational Resilience. This Topical Requirement and user guide give auditors a framework to evaluate governance, risk management, and controls that support resilience amid sudden disruptions and long-term pressures. **theiia.org/tr-org-resilience**

GLOBAL TECHNOLOGY AUDIT GUIDE

IT Change Management. This guide and its companion tools help internal auditors explain change management's growing complexity, ask questions, identify leading practices, and assess controls. **theiia.org/gtag-it-chge-mgmt**

GLOBAL PRACTICE GUIDE

Data Analytics Guidance and Resources for Internal Auditors. This suite of two global practice guides and a maturity model helps auditors understand analytics, build critical skills, and plan a practical path toward more data-driven assurance. **theiia.org/gpg-data-analytics-ia-resources**

GLOBAL SURVEY

State of the Standards Survey. The IIA invites members to share information about how they conform with the Standards and Topical Requirements. The findings will help guide The IIA's future resource development. **theiia.org/state-standards**

What's Trending

GLOBAL PRACTICE GUIDE

Coordination and Reliance: Working With Other Assurance Providers. This practice guide outlines how CAEs can align risk assessments and coordinate with other assurance providers. **theiia.org/developassurancemap**

IIA AUDIT TOOL

Coordination and Reliance: Assurance Mapping. This tool includes an example assurance map for working with other assurance providers plus a customizable blank version. **theiia.org/tool-coord-reliance-assurance-map**

IIA AUDIT TOOL

Coordination and Reliance: Reliance Assessment. This tool illustrates how to assess and document the basis for the level of reliance that internal audit can place on the work of other assurance providers. **theiia.org/tool-coord-reliance-assessment**

IIA AUDIT TOOL

Model Internal Audit Charter Tool and User Guide. This updated tool helps internal audit functions customize their audit charters while conforming with the requirements of Standard 6.2 Internal Audit Charter. **theiia.org/auditmodel**

Coming Soon

GLOBAL PRACTICE GUIDE

Evaluating the Effectiveness of Ethics Programs. This guide and companion tool help internal auditors assess whether ethics programs meet objectives and are embedded in governance, risk management, and operations.

TOPICAL REQUIREMENT

Anti-Corruption. This Topical Requirement details what internal auditors must do when assessing an organization's anti-corruption program. The draft for public consultation opens in June in multiple languages.

community

Highlights

IIA–Puerto Rico Named Ruby Chapter

The IIA–Puerto Rico Chapter recently became the first Caribbean chapter to earn the Ruby Chapter designation for 10 consecutive years of Gold status under The IIA's Chapter Achievement Program. This milestone reflects the chapter's excellence in education, leadership, and member engagement.

13 Schools Join Internal Audit Academic Alliance

The IIA and the Internal Audit Foundation have added new schools to the Internal Audit Academic Alliance, which recognizes universities that introduce students to internal auditing and offer dedicated coursework.

- *Ana G. Méndez University*, Orlando, Fla. campus
- *Bahçeşehir University International*, Istanbul, Turkey
- *Bow Valley College*, Calgary, Alberta
- *Bryant University*, Smithfield, R.I.
- *College of Banking and Financial Studies,* Muscat, Oman
- *Nanjing Audit University Jinshen College,* Nanjing, China
- *Oregon State University*, Corvallis, Ore.
- *Rutgers University*, Newark, N.J.
- *Southern Illinois University*, Carbondale, Ill.
- *Tampere University*, Tampere, Finland
- *The Ohio State University*, Columbus, Ohio
- *United International University*, Dhaka, Bangladesh
- *University of Illinois Urbana-Champaign*, Ill.

IIA–India & ICMAI Launch CIA Pathway

IIA–India and the Institute of Cost Accountants of India (ICMAI) have signed a memorandum of understanding that enables Certified Management Accountants to earn the Certified Internal Auditor (CIA) designation through the CIA Challenge Exam.

Career Moves

Elizabeth Sullivan, CIA, CRMA, CCSA, former IIA North American Board Chair and chief risk and audit officer at the Washington Metropolitan Area Transit Authority, has been named one of *Washington Business Journal*'s Diversity in Business Award recipients.

Maciej Piołunowicz, CIA, member of IIA-Poland, has received the Copernicus Medal from the Polish Bank Association, the highest distinction in Poland's banking sector, for his lasting contributions to the Global Internal Audit Standards.

Adrian A. Romero, CIA, CRM, IIA–Miami Chapter President, has joined Kaufman Rossin as a principal in its Risk Advisory practice, where he will lead the practice and support clients in navigating risk.

Faisal Almuraykhi, CIA, CRMA, CISA, CFE, member of IIA–Saudi Arabia, has started a new position at stc as internal audit director.

Calendar

JULY 11

RISE Virtual Conference

JULY 20–22

In-Person IIA Learning Seminars, Phoenix

AUG 19–21

IIA–Costa Rica XXVI Internal Audit Congress, San José

A conference bringing together auditors and governance leaders to share practical insights and strengthen audit maturity across organizations.

AUG 26–28

IIA–Colombia XVIII Internal Audit Congress, Barranquilla

National congress connecting internal audit leaders for a three-day program.

OCT 15–16

ECIIA Conference, Brussels

European conference for senior internal audit leaders, regulators, and governance experts focused on artificial intelligence, sustainability, emerging risks, and leadership in disruptive environments.

SUBMIT YOUR ACHIEVEMENT

IAm *Filipe Ribeiro*

stats

CIA, CRMA, CFE

Internal Audit Manager / Al Dahra / Abu Dhabi

IIA–Brazil / Member since 2008

I'm drawn to staying active, especially around the water, which is more than just exercise for me — it's a way I switch off from my daily routine. Growing up in Rio de Janeiro, I swam regularly and later took up kitesurfing. What started as something casual quickly became a passion.

My most challenging kitesurfing experience happened in Angola. Offshore, my kite fell into the water, and the wind completely died. Unable to relaunch it, I had to swim to make it back safely. In less-developed spots, you have to be self-reliant and know your limits.

Since moving to Abu Dhabi in 2024, I've traded the ocean for the desert, where I enjoy off-roading. Driving across dunes with no strict plan, it's just you, the car, and the desert — a simple way to reset.

Between swimming, kitesurfing, and off-roading, staying active brings balance outside of work. It also mirrors what I value in internal auditing: staying alert, adaptable, and comfortable with uncertainty.

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

Deloitte.

Unlock the full potential of your internal audit function

We advise clients on how to build, manage, augment and transform their internal audit functions. We serve as our clients' internal audit department to enhance the effectiveness and efficiency of this critical function.

Visit to learn more