2025

Focus on the Future

Inflection Point for Transformation at Mid-Decade

Richard Chambers

Table of Contents

Introduction: Internal Audit Stands at a Mid-Decade Crossroads	3
Top Takeaways From the 2025 Focus on the Future Survey	5
AI Use and Governance: An Alarming Lack of Progress	6
Standards Implementation: A Lack of Readiness Amid Lingering Challenges	12
2025 Top Risks: Static Views of a Dynamic Risk Landscape	19
Audit Effort vs. Risk: Persistent Misalignment on Key Vulnerabilities	24
Resources and Talent: Risk Grows While Resources Stagnate	30
Internal Audit at Mid-Decade: An Inflection Point	36
Methodology and Participants	38
About the Author	39
About AuditBoard	39

INTRODUCTION

Internal Audit Stands at a Mid-Decade Crossroads

The first half of the 2020s has been an era of perpetual risk-induced disruption — an age of permacrisis that is unrelenting. Amid these volatile conditions, organizations' ability to identify, understand, and manage their key risks is essential for resilience, performance, and agility. **But as risk grows, risk resources aren't keeping pace.** They're shrinking or stagnating for most organizations. The challenge is to drive better results from existing resources.

The internal audit profession is struggling to meet the need. It hasn't seen meaningful growth in almost 20 years. It is stagnant at best, with an aging workforce and fewer people entering the field. This contributes to a widening gap between rising risk volume and organizations' capacity to manage their risks — the "risk exposure gap."

Despite the obstacles, internal audit leaders face a critical imperative to help their organizations tackle the gap head-on, by improving how they strategize, prioritize, use technology, manage talent, and collaborate across the organization. Unfortunately, as AuditBoard's 2025 Focus on the Future survey shows, some CAEs are missing key opportunities to narrow the gap. AuditBoard surveyed 376 global internal audit leaders in August 2024, and the data reveals:

- **A startling lack of progress in implementing generative AI in internal audit,** imperiling our objective of being valued as a trusted source of assurance on risk management and increasing our risk of being marginalized by AI. Fortunately, as our report details, there are several straightforward ways internal auditors can start leveraging AI.
- **Underestimated AI risk paired with a lack of understanding of AI usage,** suggesting potentially inadequate risk assessment and monitoring in this fast-expanding risk area — and pointing to a prime opportunity for internal auditors to step up.
- **Lack of readiness to conform with The Institute of Internal Auditors' (IIA's) *Global Internal Audit Standards* (Standards),** a troubling indication of the lack of priority some internal auditors may be placing on professionalism and quality assurance.
- **Immature views on the process, purpose, and importance of internal audit strategic planning and technology planning,** reflecting the need for greater foresight and increased collaboration with other risk and assurance teams.
- **Ongoing misalignment between risk levels and audit efforts in key areas,** suggesting seemingly static views on risk and resource allocation while highlighting potential opportunities to reprioritize, redirect, and achieve efficiencies.
- **Persistent optimism about internal audit budget and headcount,** despite ongoing economic uncertainty and historical evidence to the contrary.
- **A watershed opportunity for internal auditors to become agents of change** in key governance, risk, and compliance areas impacting our organizations, including AI and other emerging technologies, organizational culture, strategic planning, talent, and more.

Our organizations have experienced a half-century's worth of disruption in half a decade. These are not ordinary times; extraordinary action is required. In too many instances, however, it appears that internal auditors are still struggling to maintain a focus on the most significant risks to their organizations and aggressively adapt to the new risk reality. Internal audit's traditional cautiousness — including our perennial hesitancy to adopt new technologies and approaches — will not serve our profession or our organizations well in the second half of the decade.

The internal audit profession is facing an inflection point. We must better equip ourselves to understand and face tomorrow's risks while driving more benefit from limited resources. That requires thinking and working in new ways. We've made only tepid progress, but today's risk conditions demand real evolution through purposeful transformation. 2025 Focus on the Future offers hard lessons. Fortunately, they point to vital opportunities on the path to transformation.

Top Takeaways From the *2025 Focus on the Future* Survey

The future is always uncertain. We still have to prepare for it.

A persistent state of permacrisis requires internal auditors to become better at anticipating, identifying, and monitoring increasingly volatile risks. Are you prepared?

Ongoing optimism about resources is rarely realized.

6%

expected headcount decreases in 2024.

11%

experienced headcount decreases in 2024.

Misalignment continues between audit efforts and key risks facing the organization.

#2 RISK #11 AUDIT EFFORT

Changing economic conditions.

High risk level, low planned 2025 audit coverage.

#10 RISK #3 AUDIT EFFORT

Fraud.

Low risk level, high planned 2025 audit coverage.

IIA Standards implementation: At least one in three organizations won't be ready.

Implementing the *Standards* is no small task, and the Topical Requirements will make conformance a moving target.

35%

do not expect to fully implement the Standards by the January 2025 deadline.

42%

of small internal audit functions (≤6 FTEs) expect to miss the deadline.

41%

say strategic planning isn't critical enough to displace other responsibilities.

AI use and governance: An alarming lack of progress and a parade of red flags.

Many CAEs underestimate AI's risk and impact — while acknowledging how little they understand or use it.

#14 RISK

Organization's use of AI.

Ranks lowest of all risks in the 2025 survey.

32%

believe AI will significantly transform internal audit processes.

4%

report substantial progress implementing AI in any area of internal audit.

AI Use and Governance: An Alarming Lack of Progress

Overconfidence has no place in risk management. You will gain — and deserve — more respect if you demonstrate humility about what you don't know and make a plan to remedy it. Unfortunately, many CAEs seem unable to help their organizations understand AI and its risks.

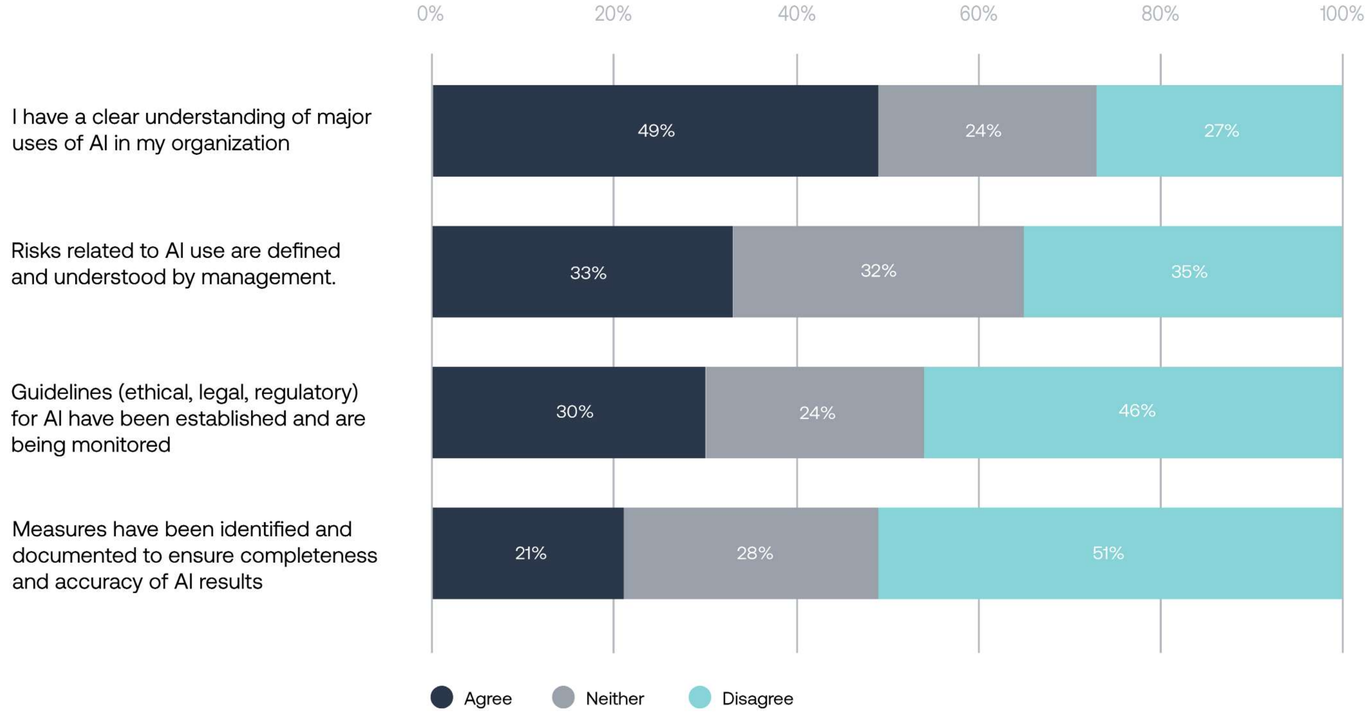
I theorize that the more someone learns about AI, the less likely they are to think they're any sort of expert. **That's why it's worrying that so many internal audit leaders admit their lack of AI expertise while simultaneously diminishing AI's risks.** As I called out in the top takeaways, of the 14 risks listed as possible choices in the 2025 *Focus on the Future* survey, internal audit leaders collectively ranked "organization's use of AI" as the lowest.

Certainly, the AI landscape is constantly evolving, and our grasp of its uses and risks is continually unfolding and maturing. **Nobody is an "expert" yet — boards, management, and regulators are all struggling to keep pace.** This is precisely why internal auditors should dive in headfirst and make a deliberate and ongoing effort to learn about AI technologies, risks, and governance. Understanding the current state offers a clearer picture of the road ahead.

Organizational Use and Governance of AI

As Figure 1 reflects, most CAEs report that their organizations' AI governance — as well as their understanding of their organizations' AI usage or risks — significantly lacks maturity.

(FIGURE 1) *Organizational Use and Governance of AI*



KEY QUESTION

Is a large segment of the internal audit profession truly failing to understand how AI is being used in their organizations? These results suggest that most CAEs have the opportunity to do significantly better. In a world and workforce being reshaped by AI's impact, I see this as a massive red flag for internal audit's future. Effective risk management is not possible without first having a baseline understanding of the risk.

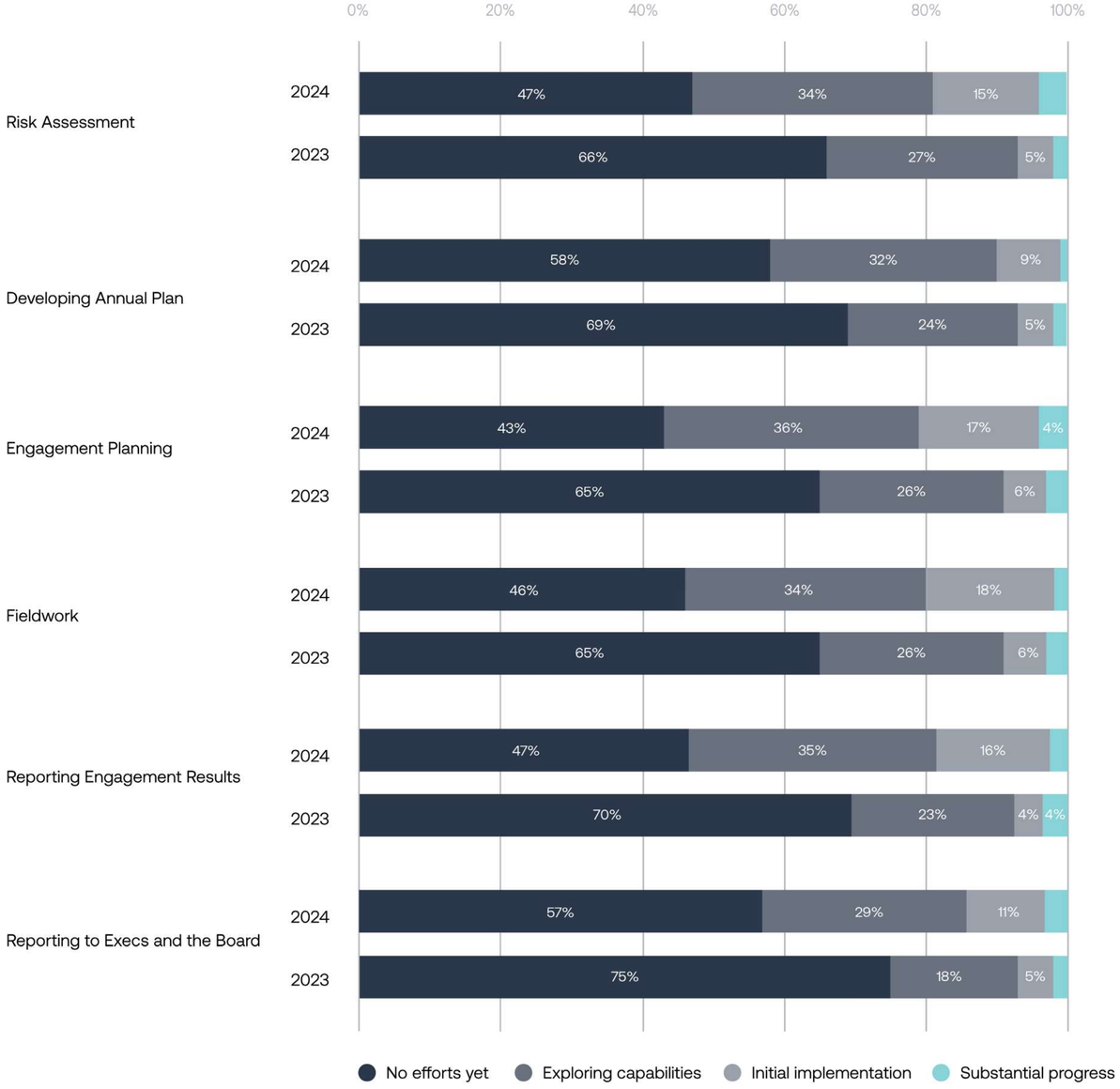
- **Just under half of internal audit leaders report having a clear understanding of the major uses of AI in their organizations.** This is a startling finding, as it would seem to suggest inadequate risk assessment and monitoring.
- **Only one in five organizations has identified and documented measures to ensure the completeness and accuracy of AI results.** The larger the department (especially in functions with ≥15 FTEs), the higher the likelihood they have established AI guidelines and identified and documented measures for ensuring completeness and accuracy.

Internal Audit Use of Generative AI

The 2025 *Focus on the Future* survey also examined how internal auditors are using generative AI in their own work. Unfortunately, as Figure 2 shows, internal audit's use of generative AI also appears to be highly immature.

- **Approximately half of all internal audit functions have made no efforts toward implementing generative AI in any part of their work.**
- **Only 4% of functions report substantial progress in implementing generative AI in any area.** Fewer than 1 in 10 report any progress in using AI to develop the annual internal audit plan, and approximately 1 in 5 report the same for engagement planning, reporting engagement results, fieldwork, or risk assessment.
- **The good news: The number of internal audit functions reporting any progress in implementing AI doubled from last year's survey in many cases.** However, that progress doesn't impress when you know that the biggest jump is from 9% to a mere 21% implementation (in engagement planning).

(FIGURE 2) *Internal Audit's Current Use of Generative AI*



The lack of progress since 2023 is disappointing, especially given that last year's survey set a low bar. The *2024 Focus on the Future* report found that, **at most, 10% of internal audit functions were using generative AI in any way in 2023, and 65–75% had not yet put any effort into exploring or implementing generative AI**. Notably, this figure lags far behind the AI usage reported in the working world at large. A 2024 CompTIA survey of 500+ technology industry professionals found that 55% of organizations are either aggressively pursuing integration of AI (22%) or undertaking limited implementation (33%).

Data breakdowns by industry and function size yield a few more noteworthy insights:

- **Finance organizations lag behind other industries in every area.** This may reflect the industry's more regulated nature, with internal auditors cautious about implementing new technologies until they've been formally approved by regulators.
- **Services and technology organizations report slightly greater progress in most areas.** This isn't surprising, as these industries tend to be early adopters of new technologies.
- **Larger teams are more likely to have implemented AI.** While this finding is encouraging, smaller functions may more quickly realize substantial benefits from AI implementation. After all, a team of 100 internal auditors doesn't need AI as a capacity multiplier in the same way as a team of only five to ten. Unfortunately, smaller teams are also more likely to feel they don't have enough staff to work on AI implementation.

KEY QUESTION

Why aren't more internal auditors taking meaningful action toward implementing AI in their day-to-day work?

I've been a highly vocal champion for generative AI, so I've been approached by countless internal auditors who call out the obstacles they face in adoption. Many point to their organizations' strict regulations on AI usage. Others stress the need to exercise caution. Both are valid reasons to take care. Neither is an excuse to fail to make any progress whatsoever. **Remember, your acumen, judgment, and experience are your safety net.**

Others feel too busy to plan and innovate in this area. The irony is that **AI holds incredible potential as a capacity multiplier and work accelerator for internal audit, helping resource-strapped teams achieve better results with less effort**. We'll take a closer look at internal audit's use of capacity multipliers later in the report.

Internal Audit's AI Outlook: A Credibility Gap Emerges

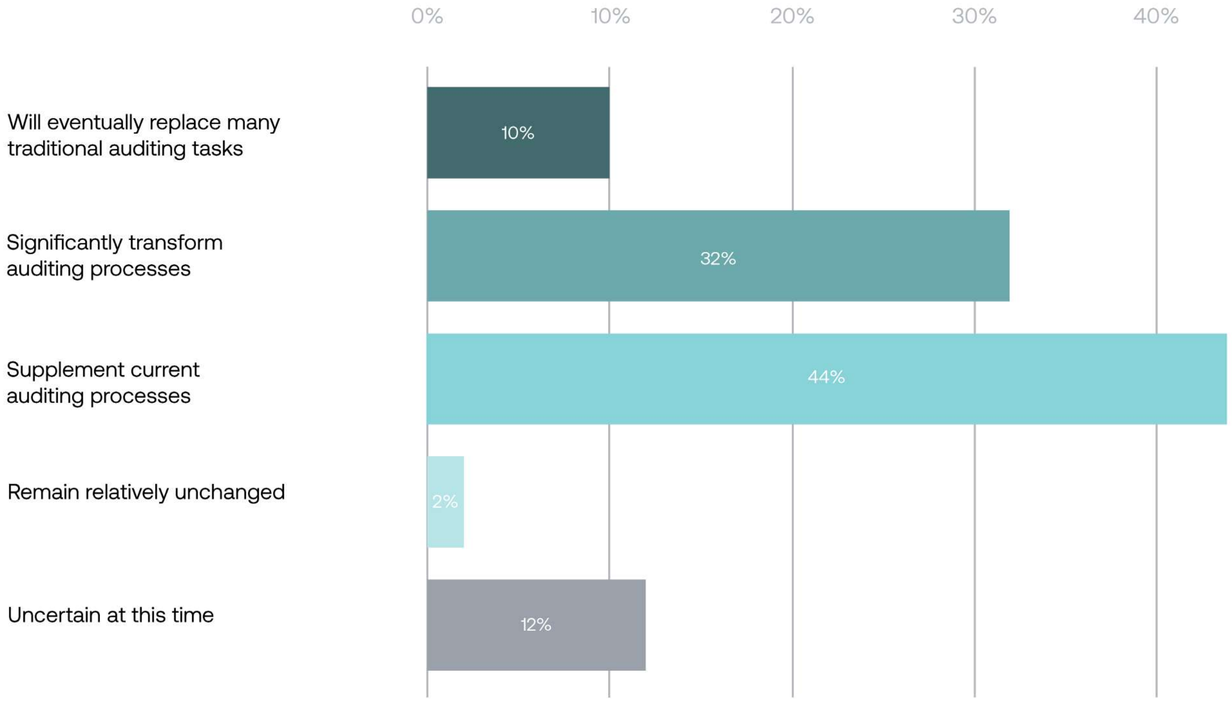
Internal auditors must follow the risks to focus on the future. This fundamental truth is the inspiration behind this annual report's title and purpose. Unfortunately, based on the 2025 survey, **I fear that many internal auditors' focus may be severely lacking when it comes to the future of AI and the risks it creates**.

One root of the problem: Many internal auditors simply don't understand how AI can be used to improve their work, so they underestimate AI's likely impact on the future of the profession. We asked CAEs how they foresee AI evolving in internal audit over the next five years. As indicated in Figure 3, **most view AI merely as contributory — not revolutionary**.

- **Just under half of respondents (44%) think AI's biggest role will be in improving what they are already doing**, primarily supplementing current processes.
- **Slightly fewer (42%) see AI's potential for transformative change:** 32% anticipate significant transformation and 10% think AI will eventually replace many traditional tasks.

Interestingly, smaller internal audit functions express both higher levels of uncertainty and stronger beliefs that AI will replace traditional internal auditing tasks.

(FIGURE 3) *Expected Role of AI in Internal Audit, Next Five Years*

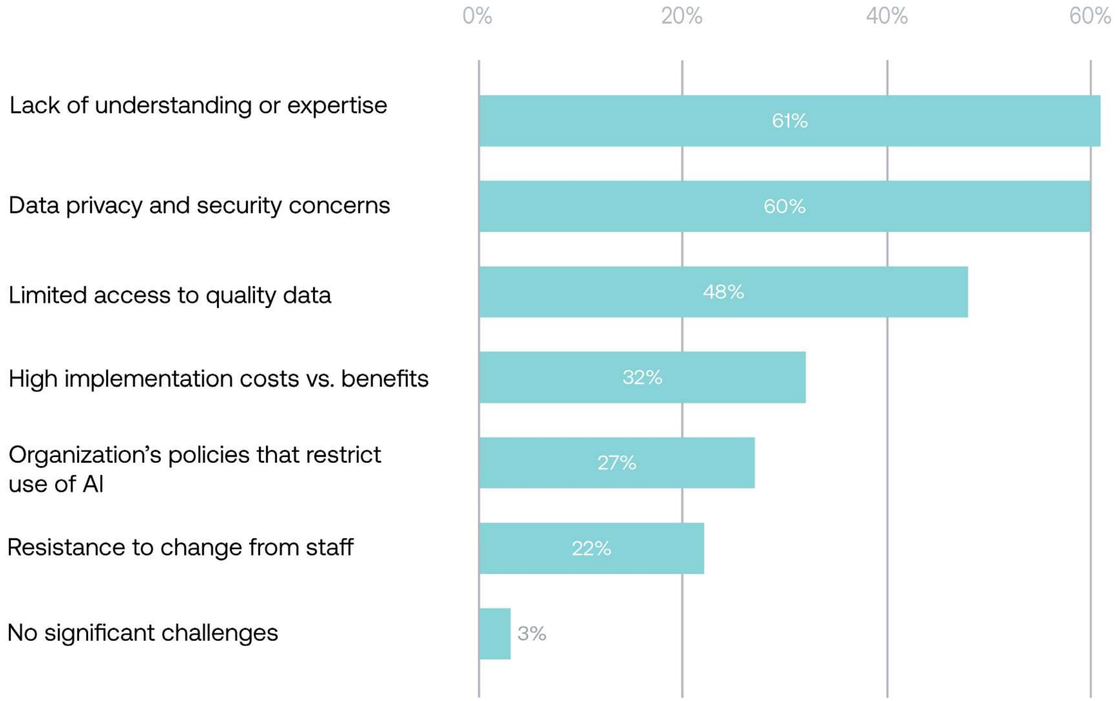


KEY QUESTION

It's undeniable that AI will have a transformative impact on internal audit. So I can't help worrying: **Are many internal auditors significantly underestimating AI's impact primarily because they do not understand AI's capabilities?**

When CAEs identify all of the challenges they face in implementing AI within internal audit, their responses seem to validate this theory. As Figure 4 shows, a resounding 61% point to a shortfall of AI understanding or expertise. **If this many CAEs readily admit that they lack understanding or expertise in AI, how credible are their predictions about AI's future impact on the profession?**

(FIGURE 4) *Challenges to Internal Audit Implementation of Generative AI*



KEY QUESTION

We must address the elephant in the room: Internal audit has an emerging credibility gap when it comes to AI. **Why should our organizations listen to our predictions about AI if we simultaneously admit we don't know much about it?**

Internal audit will unquestionably be transformed by AI's impact. Potential use cases span everything from research, report creation, risk assessment, documentation (e.g., risk or issue authoring), audit planning, framework adoption, and routine task automation to continuous risk monitoring, fraud prevention and detection, certain testing and scanning tasks, and so much more. Instead of burying our heads in the sand, we must embrace this opportunity to define our profession's future.

We can do this by taking action to understand and use AI. Without cultivating this understanding, we can't hope to earn a seat at the table for this urgent conversation. What's more, we increase the risk that AI could challenge our profession's very existence.

Future-Focused Auditor Tip

Take meaningful action to learn about and implement AI within internal audit. While it's obviously essential to ensure that your efforts align with organizational policy (e.g., data privacy requirements), there are several ways you can get started. For example:

EDUCATE YOURSELF ABOUT AI TOOLS AND PROMPTS.

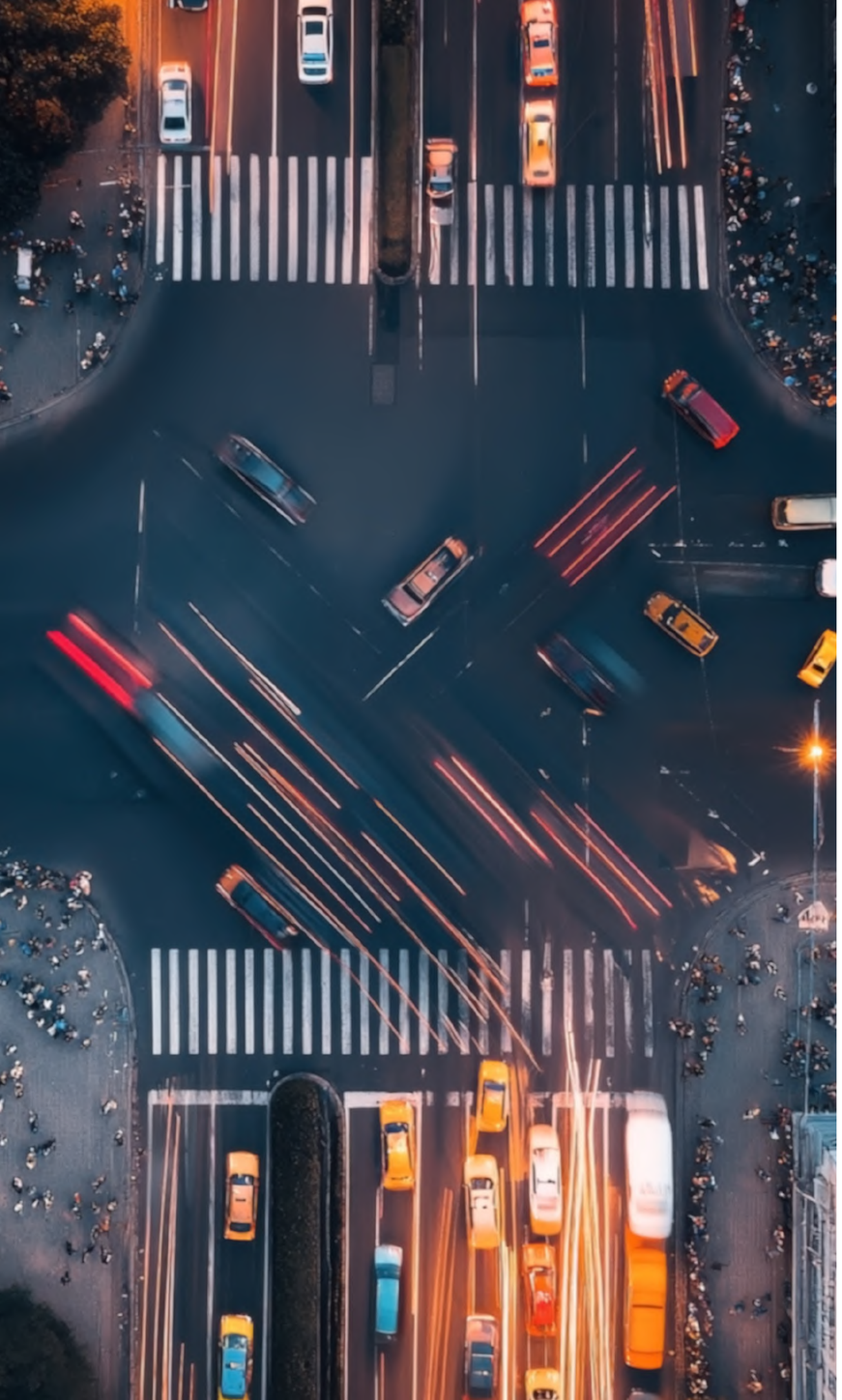
The more you use generative AI tools, the better you'll understand their potential benefits and limitations. Learning to write effective AI prompts is a key skill. The more specific and detailed your prompts, the better results you're likely to get. You can also provide an example of the output you want, either by asking the AI tool to model its output on your example or edit the example you provide.

EXPERIMENT WITH USING AI IN PROVEN AREAS.

- Risk assessments may be the easiest place to start. AI tools can quickly produce initial research on key risks for 2025, offering a great starting point for your research. Try different prompts based on your industry, organization, function size, or other variables.
- Fieldwork and reporting offer many opportunities to try out AI tools, which can analyze data, automate tasks, suggest procedures, generate summaries, expedite report writing, check compliance, or otherwise assist with planning, assessments, and reporting.

SEEK OUT OPPORTUNITIES TO EXPAND YOUR AI EDUCATION.

- **Research the potential for AI-powered data analytics.** These can be game-changing capacity multipliers for testing, scanning, process mining, surfacing predictive insights, creating data visualizations, and more. Work with your IT function to identify and evaluate potential technologies.
- **Look for AI capabilities in existing audit, risk, and compliance technologies.** For example, you may uncover AI-driven accelerators for project management, control mappings, identifying duplicate requests, staffing, drafting and summarizing reports, issues, and risk descriptions, and more.
- **Seek out leading practices from other internal auditors.** The IIA's dedicated AI knowledge center, LinkedIn articles or forums, AI newsletters, YouTube, networking, and technology-focused blogs like AuditBoard's are excellent places to look (e.g., Faisal Shafiullah's recent article sharing practical use cases).
- **Take formal AI training courses.** Of the many AI upskilling resources internal auditors might leverage, The IIA offers several hands-on online courses focused on helping practitioners leverage AI tools in their work, audit organizational use of AI, and more. ISACA also offers training customized to different ability levels.
- **Learn about AI governance.** This World Economic Forum article offers an overview and links to helpful guidance (e.g., NIST's AI Risk Management Framework).



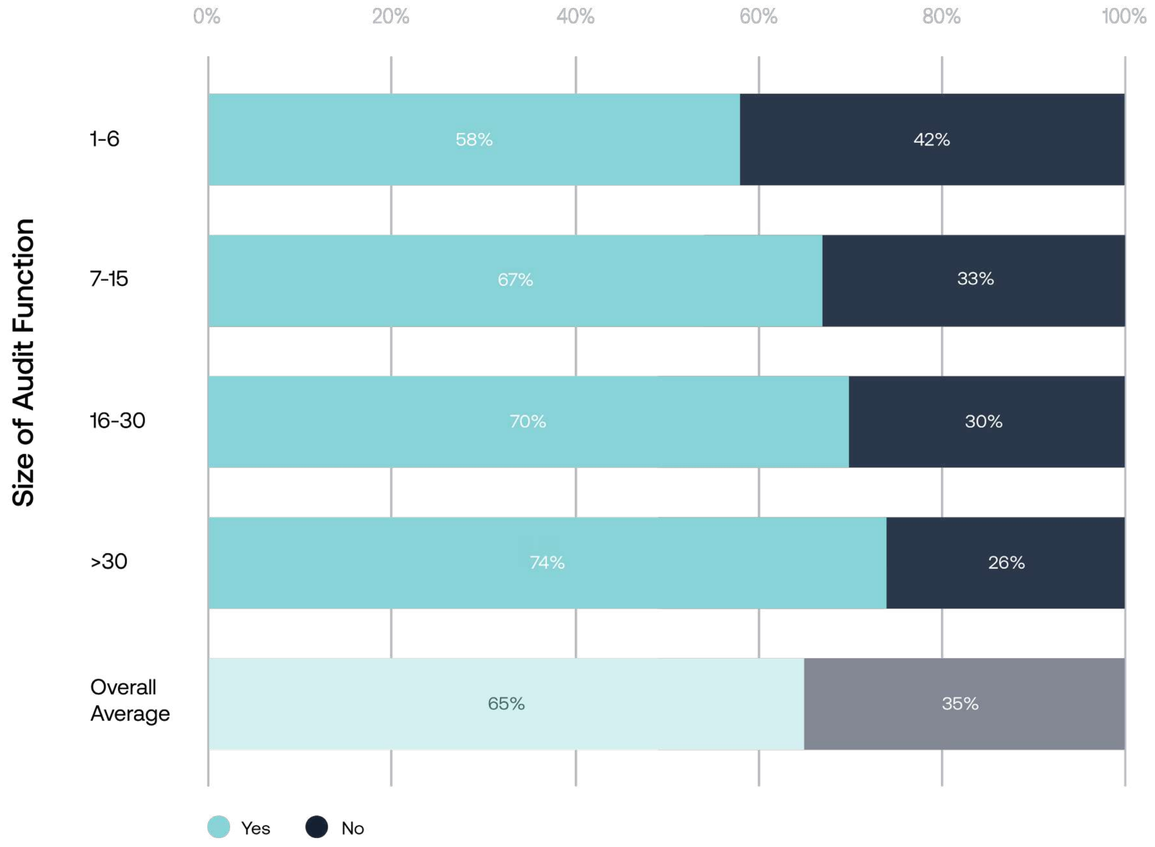
Standards Implementation: A Lack of Readiness Amid Lingering Challenges

The IIA released the new *Global Internal Audit Standards* in January 2024; they take effect January 9, 2025. The Standards include many noteworthy changes, including:

- **Increased prescriptiveness**, requiring CAEs' detailed review to confirm that practices reflect requirements and update them as needed.
- Greater emphasis on internal audit **strategy, relationship-building, communication, and technology planning**.
- **New emphasis on performance management**, requiring CAEs to develop and assess objectives to evaluate performance and embed quantitative metrics in strategic plans.
- **Raised bar on both internal and external quality assessments**, requiring CAEs to consider conformance with Standards and achievement of performance objectives.
- **Less differentiation between assurance and advisory requirements**, which may prove challenging for CAEs who provide a variety of advisory services.
- **New Topical Requirements**, created to ensure consistent internal audit methodologies for assessing governance, risk management, and controls effectiveness for specific topics.

In other words, implementing The IIA's new Standards is no small matter. Nobody is suggesting otherwise. What's more, the Topical Requirements, which will be issued over time, will make overall Standards implementation an ongoing exercise as functions may struggle to keep up. Unfortunately, as Figure 5 reflects, **more than one-third of internal audit leaders believe they will not be ready for the first big hurdle**.

(FIGURE 5) *Expected IIA Standards Implementation by 2025 Deadline*



- **Among all respondents, 35% do not expect to meet the January 9, 2025 deadline.**
- **Larger organizations are more likely to say they expect to meet the deadline.** This isn't surprising, given larger organizations tend to have more internal audit resources.
- **42% of small internal audit functions (≤6 FTEs) expect to miss the deadline.** If this is representative of the profession overall, up to half of small functions could fail to conform.
- **Public companies are most likely to say they expect to be in compliance; private companies are least likely.**

KEY QUESTION

If this is where compliance levels begin in 2025, how much are they likely to improve over time? The inconvenient truth: Based on my experience, the number of functions globally that will meet the deadline is liable to be even lower.

These findings are only a small piece of a much bigger picture. Regardless, the one-third expecting to miss The IIA's deadline corresponds to a large number of internal audit functions that will not be in conformance with the Standards. **This is not a healthy sign for the profession — and frankly, these low compliance levels could easily worsen in the long run, especially as more Topical Requirements come into play**.

The bottom line: Our professional standards differentiate us from other risk and oversight functions. Conformance is essential for maintaining professionalism and quality in our work.

Common Hurdles Reveal Planning Challenges — and Auditor Limitations

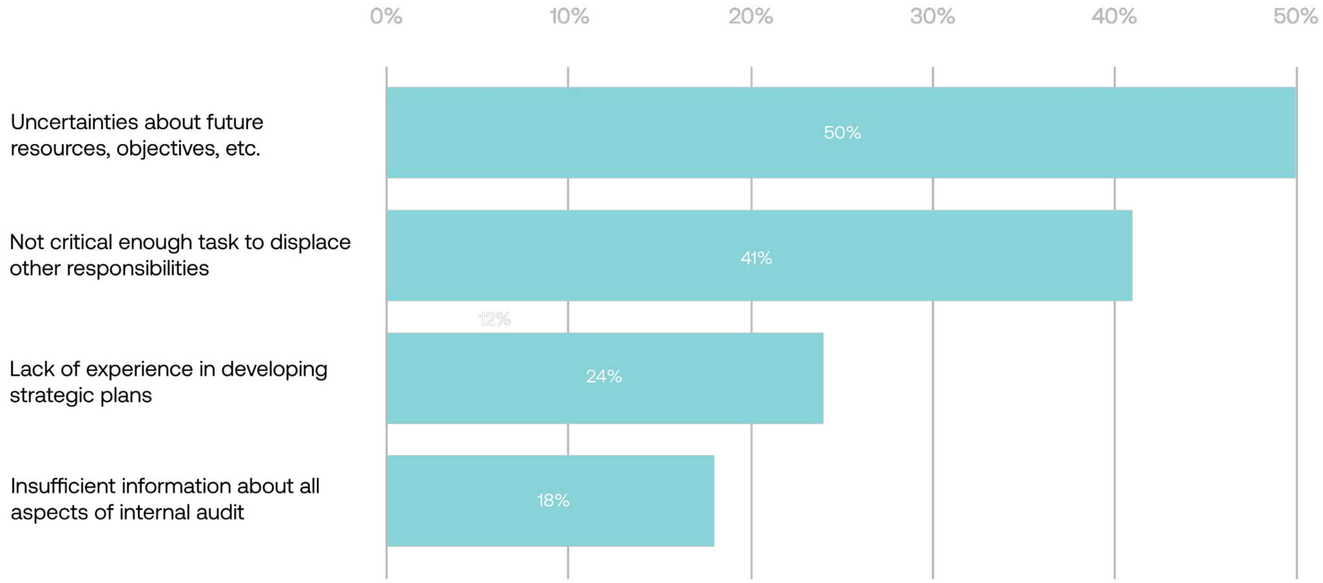
Internal auditors have had ample opportunity to air their concerns and questions since the Standards' release. Because strategic plans and technology planning are frequent topics, the *2025 Focus on the Future* survey asked respondents questions about both areas.

Strategic Planning

We asked internal audit leaders to identify any major impediments to developing the strategic plan mandated by Standard 9.2.

Most respondents identifying impediments selected only one. Unfortunately, the most common selections suggest that **many CAEs may lack a strong understanding of strategic planning**.

(FIGURE 6) *Impediments to Internal Audit Strategic Planning*



- **Encouragingly, 43% of respondents indicate "no impediments."** Figure 6 reflects the impediments reported by the remaining 57%.
- **The most commonly identified impediments suggest immature views of strategic planning.** Half of respondents cite "uncertainties about future resources, objectives, etc." and 41% say it isn't critical enough to displace other responsibilities.
- **Finance organizations are most likely to cite no or fewer impediments to developing an internal audit strategic plan.**
- **Smaller audit departments (≤6 internal auditors) are significantly more likely to report impediments.**

IIA Standard 9.2 Internal Audit Strategy — Requirements

Excerpt: "The chief audit executive must develop and implement a strategy for the internal audit function that supports the strategic objectives and success of the organization and aligns with the expectations of the board, senior management, and other key stakeholders.

An internal audit strategy is a plan of action designed to achieve a long-term or overall objective. The internal audit strategy must include a vision, strategic objectives, and supporting initiatives for the internal audit function. An internal audit strategy helps guide the internal audit function toward the fulfillment of the internal audit mandate.

The chief audit executive must review the internal audit strategy with the board and senior management periodically."

Regrettably, those who cite future uncertainty as an impediment likely do not fully understand the purpose of a strategic plan. It's precisely *because* risk is so volatile and uncertain that strategic plans are needed. As I've repeatedly stated, strategic plans aren't there to provide the answers. They exist to help you ask the right questions, identify and assess your options for responding, get everyone in your organization on the same page, and plan, prioritize, and proceed accordingly.

KEY QUESTION

If you can't make a strategic plan for your internal audit function because you have too much other work, how do you know if you are prioritizing your work correctly?

It can feel challenging to prioritize strategic planning. Smaller teams in particular tend to have a great deal on their plates. Happily, from my experience, most smaller internal audit functions can prepare their strategic plans in a fraction of the time it takes larger functions.

I am a longtime advocate for strategic planning in internal audit, so I applaud and champion The IIA's new requirements in this area. **I know the process can be intimidating, and that not all CAEs possess a naturally strategic mindset.** Some of us are more tactical, and tactical approaches can yield great benefits. However, many CAEs will have to step out of their comfort zones to satisfy this requirement.

Whatever the impediments, strategic plans are worth the time and effort. They are a key mechanism by which we can create roadmaps that help our internal audit functions to get from where they are today to where they need to be in the future, ensuring relevance, innovation, and value protection and creation. Regardless, having a strategic plan is now a must-have for conformance with the *Standards* — as well as for receiving a clean external quality assessment.

Future-Focused Auditor Tip

Challenge yourself to improve your strategic planning process. As CAEs create and refine their processes, more guidance is likely to emerge. Existing guidance includes:

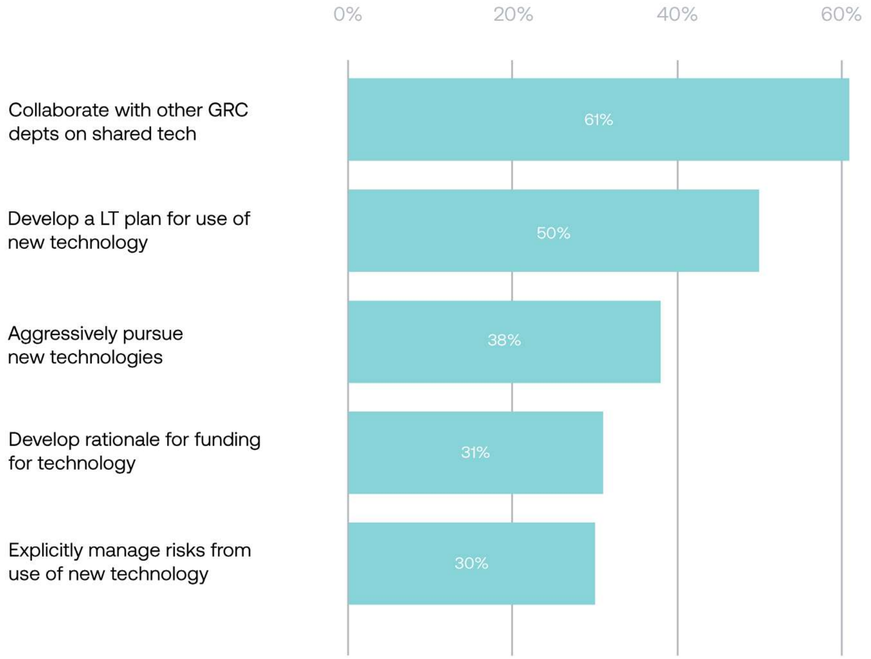
- IIA resources such as ***Implementing an Internal Audit Strategic Plan***, a range of strategic plan examples, and the practice guide ***Developing the Internal Audit Strategic Plan*** (currently being updated).
- **My 2024 blog outlining the strategic planning process I use**, which includes revalidating stakeholder needs, forging a vision statement, and planning a route (via gap analysis, formulating goals and objectives, and identifying critical success factors). I also discussed strategic planning on **Trent Russell's podcast**.
- AuditBoard's ***IIA Standards Roadmap: 6 Practical Tips to Elevate Your Audit Function***, which includes strategic plan must-haves and key questions.

Technology Planning

In the past, CAEs were simply encouraged to make effective use of technology to perform their work. Now, Standard 10.3 sets explicit expectations that the CAE will strategically use technology both within internal audit and to facilitate collaboration across the organization. **Indeed, technology is an essential component of any internal audit strategic plan.**

These are new requirements, so we wanted to know: How are CAEs solving them? As Figure 7 outlines, our findings are somewhat encouraging, as 87% of respondents indicate that they are pursuing one or more of the initiatives outlined. Overall, the larger the internal audit function, the more likely that efforts are underway.

(FIGURE 7) *Internal Audit Technology Planning Efforts*



- **Only half have long-range strategic plans for using technology in internal audit.**
- **Only 30% say they're explicitly managing risks arising from the use of new technologies.** Because cybersecurity and data privacy continue to be most organizations' top-rated risks (a finding we'll discuss in the next section of the report), this seems like a fairly obvious oversight.
- **Approximately two in five (39%) respondents are not collaborating with other governance, risk, and compliance teams to share technologies.** This missed opportunity often results in audit fatigue, duplication of effort, coverage gaps, and disconnected data and teams.

IIA Standard 10.3 Technological Resources — Requirements

Excerpt: "The chief audit executive must strive to ensure that the internal audit function has technology to support the internal audit process. The chief audit executive must regularly evaluate the technology used by the internal audit function and pursue opportunities to improve effectiveness and efficiency.

When implementing new technology, the chief audit executive must implement appropriate training for internal auditors in the effective use of technological resources. The chief audit executive must collaborate with the organization's information technology and information security functions to implement technological resources properly.

The chief audit executive must communicate the impact of technology limitations on the effectiveness or efficiency of the internal audit function to the board and senior management."

Any degree of progress is nonetheless progress. However, to make genuinely effective plans for leveraging technology, **CAEs should be undertaking efforts across all of these areas**.

KEY QUESTIONS

Internal audit strategic plans must address people, processes, and technology. Accordingly, **how can we square the 50% lacking a strategic plan for technology with the 65% who say they'll be in conformance with the Standards' strategic planning requirement?**

Even more importantly, **why are so many internal auditors overlooking significant opportunities to collaborate with other governance, risk, and compliance functions?**

My new book, *Connected Risk: Conquering the Perilous Risk Exposure Gap*, takes a deep dive into the risks and issues created by disconnected technologies and teams, as well as the benefits realized when these teams regularly share perspectives and resources, coordinate activities, and align data, definitions, and priorities. As the book asserts, **improved collaboration is vital for strengthening risk management to better meet the needs of the modern age**.

Future-Focused Auditor Tip

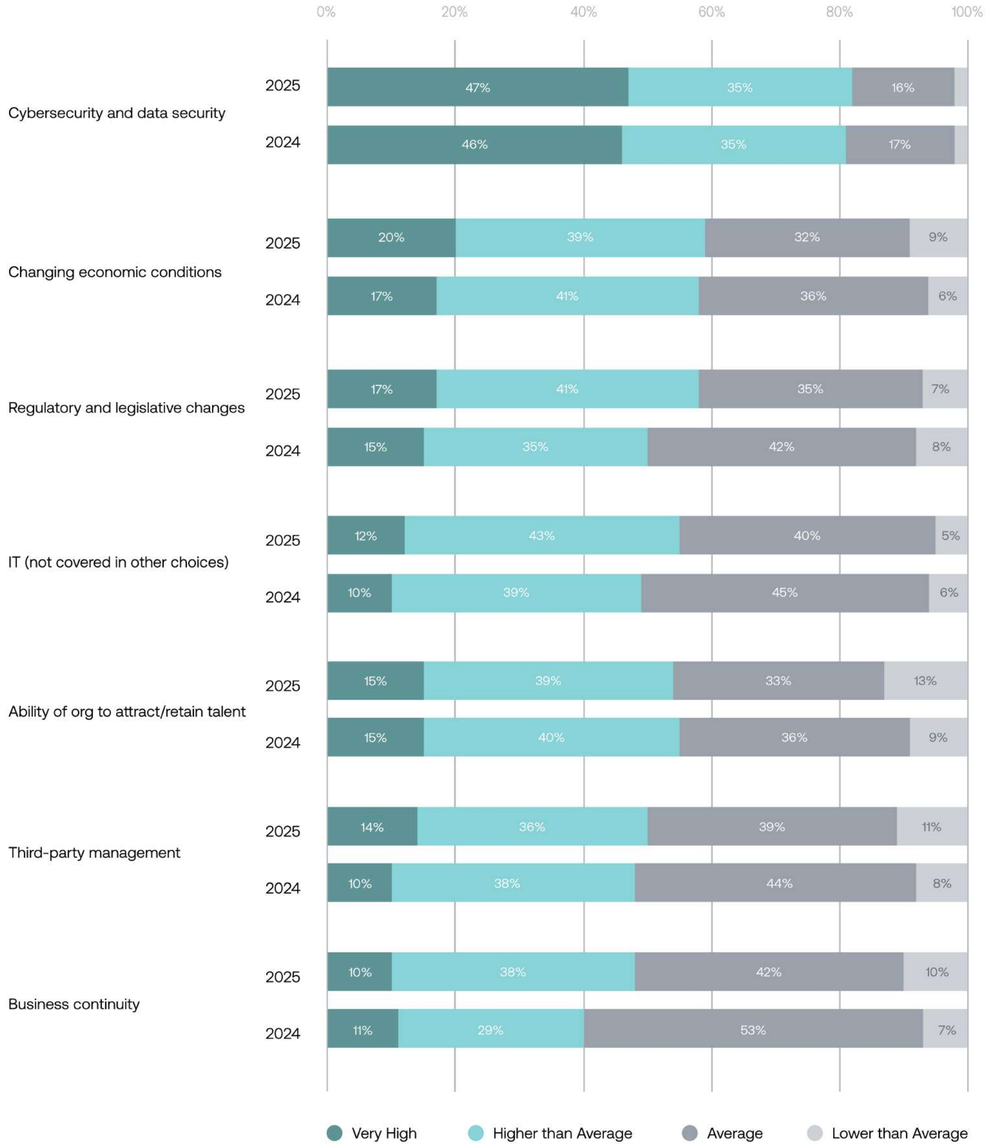
Make a detailed strategic plan for technology use in internal audit. I collaborated on a blog that includes an example strategic plan for technology and guidance on conforming with the Standards. An overview of our five-step plan:

- **Perform a gap assessment** to identify technology limitations and opportunities to improve audit project and workflow efficacy and efficiency. Follow with a feasibility assessment to determine the cost/likelihood of implementation success.
- **Collaborate with other departments** to gauge interest in implementing a connected risk platform for shared governance, risk, and control management; use of common high-powered analytics tools (e.g., SAS, Tableau); protocols for using AI; and data acquisition, cleansing, and warehousing technologies.
- **Develop a fully supported business case** for technology funding requests requiring board/management approval.
- **Develop an implementation plan** that includes measurable KPIs and milestones. Ensure compliance with organizational policies.
- **Identify and respond to technology risks specific to internal audit** (e.g., information security, data integrity, confidentiality, third-party data exposure, data retention/privacy).

2025 Top Risks: Static Views of a Dynamic Risk Landscape

Each year, Focus on the Future takes a fresh look at the risks commanding internal audit's attention. The permacrisis that began in the first half of the decade persists, creating a constantly evolving risk landscape in which challenges emerge and change faster than ever. Faced with ongoing macroeconomic and geopolitical instability, sustained increases in data breaches and other cyber crimes, new risks from AI and other emerging technologies, pervasive misinformation and disinformation, and a significant uptick in regulatory changes and scrutiny, **today's daunting risk environment presents profound risk management challenges**. Interestingly, against this backdrop, our 2025 survey suggests that internal audit leaders have a fairly static view on risks relative to last year's rankings, as seen in Figure 8.

(FIGURE 8) *Top Seven Risk Areas — 2025 vs. 2024 Rankings*



Cybersecurity and Data Security Risks Remain Dominant

Cybersecurity and data security retained top billing in internal auditors' outlook for the coming year: **82% rate this risk as "very high" or "higher than average" for their organizations in 2025**, versus 81% in 2024 and 83% in 2023. Reinforcing these findings, internal audit leaders surveyed in the Internal Audit Foundation's (IAF's) 2025 Risk in Focus reports rank cybersecurity as No. 1 for 2025 and on the three-year horizon, both globally and in North America.

Internal audit leaders are right to stay focused, because cybersecurity and data privacy are unlikely to surrender the lead ranking anytime soon. Cybercrime will continue rising, exacerbated by rapid technological advances that escalate the sophistication, automation, and reach of attacks.

In response, regulators around the globe have taken decisive actions to compel organizations to manage their cybersecurity and data privacy risks, creating significant new risk management and compliance challenges for organizations. For example:

- **U.S. Securities and Exchange Commission (SEC) cybersecurity rules now mandate that public companies disclose material cybersecurity incidents** to the SEC via a Form 8-K filing within four business days. This requires organizations to continuously monitor for cyber incidents and materiality, and assess and report any material incident within a very tight time frame. Private organizations partnering with public companies are also feeling the impact. A January 2024 AuditBoard survey of security professionals and executives found that 68% of respondents felt overwhelmed by complying with the ruling.

- **Data privacy legislation continues to proliferate.** According to United Nations Trade and Development data, 71% of countries worldwide have now enacted data protection and privacy legislation. The International Association of Privacy Professionals reports that 19 U.S. states have enacted comprehensive data privacy laws, with other states planning to follow suit. Many organizations are likely to have risk exposures in multiple jurisdictions, complicating the expanding web of data protection obligations.

Economic and Regulatory Changes, IT, and Talent Risk: Organizations Aren't Letting Their Guard Down

Survey respondents' views of other top risks also stayed fairly consistent from 2024 to 2025, despite ongoing developments in each area. Along with #1 risk cybersecurity and data security, 2024's other top-five risks largely stayed put for 2025, sometimes moving a point or two. Looking at each in turn:

- **#2: Changing economic conditions**, which ranked second for 2024, third for 2023, and seventh for 2022. The U.S. Federal Reserve System's (the Fed's) September 2024 half-percentage-point interest rate cut was the first in four years, since the early days of the COVID-19 pandemic. The cut reflected the Fed's growing confidence that it has successfully moderated inflation — as well as its ongoing concern that the economy could still slide into recession. The October 2024 jobs report has further stoked those fears, and **history shows that rate cuts sometimes precede worsening economic conditions**. Most business leaders agree, ranking "economic conditions, including inflationary pressures" as the #1 risk in 2024 and #7 risk on the 10-year horizon, according to Protiviti and NC State University's *Executive Perspectives on Top Risks 2024-2034*.

- **#3: Regulatory and legislative changes**, climbing slightly from prior-year rankings: fourth for 2024, fifth for 2023, and fourth for 2022. The pace of change has continued to accelerate throughout 2024, and it shows no signs of abating. **Regulatory scrutiny and activity keep rising in areas such as sustainability, cybersecurity, and data privacy, with potential laws to regulate AI and social media looming on the horizon.** KPMG's *2024 Global Chief Ethics and Compliance Officer Survey* found that 84% of CCOs expect regulatory expectations and scrutiny to continue rising over the next two years.

- **#4: Aspects of IT not covered in other choices**, up from fifth for 2024, the first year it was offered as a survey option. IT risks span every aspect of the organization, tying into and impacting other key risks such as top-ranking cybersecurity and data security, third-party risk management (#6 for 2025), business continuity (#7 for 2025), and "business disruption due to digitalization or other new business models" (#8 for 2025). Data management in particular is a fast-growing burden as organizations strive to ensure the security, quality, availability, and confidentiality of their data. Shadow IT — and now shadow AI, an umbrella term for AI technologies implemented without the knowledge or oversight of organizations' central IT functions — remain problematic. **As our legacy technology systems continue to age, these risks will only increase:** *Executive Perspectives on Top Risks* ranks "existing operations and legacy IT infrastructure unable to meet performance expectations as well as 'born digital' competitors" as a top-10 risk for 2025 and 2035.

- **#5: Ability to attract and retain talent**, a small decline from its #3 ranking for 2024 and #2 ranking for both 2023 and 2022. Unsurprisingly, government respondents tend to rank this risk most highly, given that government salaries and opportunities often struggle to remain competitive. Though the U.S. job market remained remarkably strong through much of the year, recent jobs reports have been inconsistent. This could be good news for employers — or it could signal a softening economy, decidedly not good news for employers' *businesses*. Most internal audit leaders still see the risk as imminent. The IAF's *2025 Risk in Focus — North America* report cites human capital risk as #2 overall for the second year running.

Rising Risks, Too Often Underestimated: AI, Culture, and ESG

While the top five risks essentially held from 2024 to 2025, the low ranking of other risks is worth noting. **Internal audit leaders may be overlooking or underestimating these critical areas.**

#11: Organizational Culture

Only 36% of respondents rate their organization's culture risk as very high or higher than average for 2025. This is a continued drop from 2024 (38% of respondents) and 2023 (46%). And yet, culture continues to be one of the most substantial yet overlooked risk concerns in any organization.

Culture can make or break **an organization.** It's not hard to think of examples both positive (e.g., Zoom, NVIDIA, Figma, Patagonia, Zappos, Netflix) and negative (e.g., FTX, Enron, Theranos). AI also is impacting culture: 34% of internal audit leaders surveyed in *2025 Risk in Focus — North America* rank organizational culture as a top-five area where AI has the most negative impact. That's more than one in three. **So why aren't all internal auditors prioritizing this risk more highly?**

Culture impacts nearly every area of risk management and organizational transformation, and can be an underlying cause of countless issues. In many cases, directly addressing problems in an organization's culture can be the only lasting way to prevent these issues in the future. **Addressing culture issues only as they arise is merely a bandage approach. It may stop the bleeding and conceal the wound, but it may not prevent the wound from opening again.**

#13: ESG

For the second year in a row, CAEs rank ESG #13 among the 14 risks listed. Only organizations with a strong environmental focus (e.g., industrial) tend to rank ESG as a top priority.

Recognition of ESG-related issues grew throughout the first half of the 2020s. Today's organizations face a widening range of ESG risks, from near-term physical risks that could damage infrastructure and disrupt supply chains to longer-term impacts, such as resource scarcity and rising temperatures. At the same time, **stakeholder expectations (e.g., customers, regulators, investors, governments, communities, employees) continue to rise**. The ESG risk disclosure landscape transformed as a result, with the simultaneous implementation of ESG-related reporting standards and requirements in the U.S., EU, UK, and globally.

Unfortunately, as *2025 Risk in Focus — North America* details, climate change risk tends to fall victim to the "tyranny of the urgent" in many organizations. **Until a risk is seen as imminent, most organizations won't act.** Unfortunately, the timing of the impact is hard to predict. The time to act is now.

#14: Organization's Use of AI

With CAEs ranking their organizations' use of AI as the lowest of any of the 14 survey options, **AI is not high on many CAEs' radar**. Services organizations tend to rank AI risk most highly.

Interestingly, *2025 Risk in Focus — North America* paints a different picture, though the difference could be due to the survey's different wording of the risk and framing of the question. When the IAF survey asked respondents to identify the top five risks facing their organizations, **respondents collectively ranked "digital disruption (including AI)" as third overall for 2025 (up from sixth for 2024) and second on the three-year horizon**.

AI use interconnects with top-ranking risks such as cybersecurity, fraud, human capital, and compliance, along with countless others. Further, AI adoption is far outpacing AI governance and risk management in most organizations. All this to say, this finding is another red flag relative to internal audit's lack of understanding of AI. **Following the risks means taking meaningful action to understand and use AI.**

Future-Focused Auditor Tip

Focus on improving your organization's continuous risk monitoring capabilities. In permacrisis, it is crucial for organizations to assess risk on a continual basis. This helps avoid surprises, mitigate risks, capitalize on opportunities, and adapt risk management in real time. In my book, *Connected Risk: Conquering the Perilous Risk Exposure Gap*, I detail a range of continuous risk monitoring tactics, including:

- **Key risk indicators (KRIs)**, which serve as an early warning risk detection system to help identify potential shifts in risk conditions that may impact the organization in the future. Technology enablement is imperative for effective KRI monitoring.
- **Monitoring internal and external indicators of emerging risk**, enabling organizations to monitor macroeconomic, political, geopolitical, industry, and other trends by methodically reviewing third-party research, economic forecasts, news headlines, customer and employee feedback, corporate initiatives, analytics, and so on.
- **"Shoe leather" assessments**, which involves walking around and talking with other risk and assurance professionals and members of business and functional management (or, in remote teams, doing so in a virtual sense) to understand how risks are shifting and changing.
- **Connecting the dots** by drawing on internal audit's extensive body of work, viewing separate audits as a series to gain clearer insight into the bigger picture.

I also recommend the **PESTLE model for identifying emerging risks** by evaluating political, economic, social, technological, legal, and environmental factors impacting organizations.

Audit Effort vs. Risk: Persistent Misalignment on Key Vulnerabilities

Every organization has limited internal audit resources, increasing the challenge for assessing how the organization's most significant risks are managed. **Unfortunately, *Focus on the Future* surveys over the past three years reveal ongoing misalignment between planned audit efforts and key risks.** As Figure 9 shows, in too many cases, high-ranking risks are receiving comparatively low audit coverage and low-ranking risks are receiving comparatively high audit coverage. Further, other supposed "matches" between risk ranking and audit coverage deserve reevaluation.

(FIGURE 9) *Top Seven Risks vs. Expected Audit Effort*

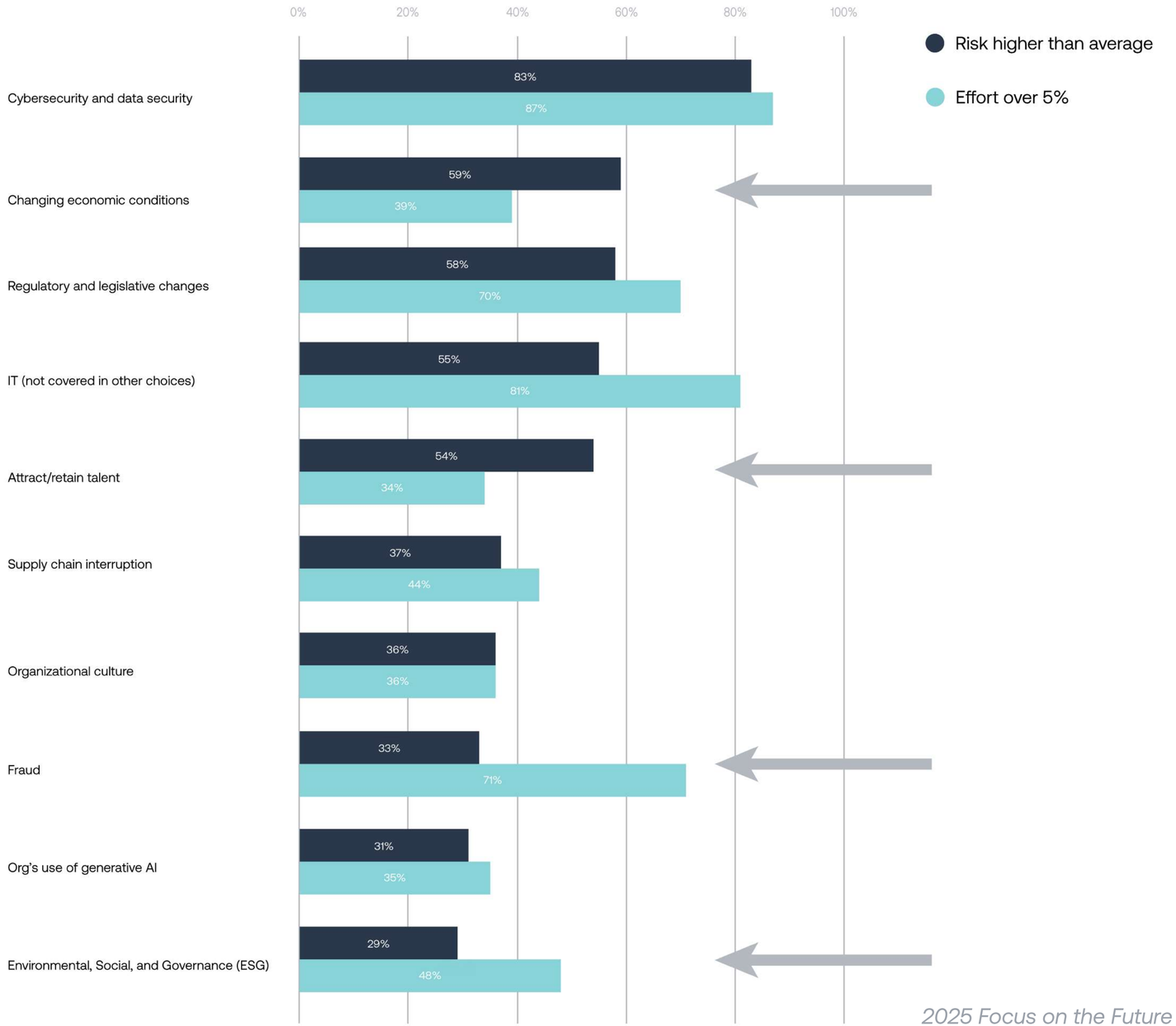
Top 7 Risks for 2025	2025 Risk Ranking	2025 Audit Coverage Ranking	>10% of Audit Effort
Cybersecurity and data security	1	1	44%
Changing economic conditions	2	11	8%
Regulatory and legislative changes	3	3	31%
IT (not covered in other choices)	4	2	34%
Attract and retain talent	5	13	6%
Third-party risk management	6	5	22%
Business continuity and crisis response	7	8	14%

KEY QUESTION

Overall, these results reveal very little change in allocation of efforts from 2024 to 2025. **Have organizations' risks really remained so consistent, or is this a case of internal auditors simply doing what they did last year — despite a dynamic and volatile risk landscape?**

Figure 10 takes a closer look at the highest- and lowest-ranking risks relative to their expected audit coverage for 2025. Major areas of mismatch become readily apparent.

(FIGURE 10) *Risk Level vs. Effort: Most Significant Mismatches*



Top-Rated Risks With Comparatively Low Audit Effort

Changing Economic Conditions: #2 Risk/#11 Audit Effort

While 59% of CAEs rank this as a top risk for their organizations, only 39% devote more than 5% of their effort and a mere 8% allocate more than 10% of their effort.

This may be a case in which internal auditors are not fully thinking through the potential impact of changing economic conditions — and thus don't see much worth auditing. After all, the first half of the 2020s was many internal auditors' first experience with the risks of inflation. The result is that many may not understand the downstream risks and are unable to adapt their methods for budgeting and forecasting, controlling expenses, adjusting prices, and managing expenses, talent, capital, and raw materials. Also inherent in declining economics is the potential for purposefully misstated financial reporting, circumvention of established purchasing policies (e.g., accepting lower-quality materials), pushing out new products before they are properly tested, and rising pressure from customers (e.g., accepting sales adjustments not approved by management), and other risks.

Ability to Attract and Retain Talent: #5 Risk/#13 Audit Effort

Although attracting and retaining talent continues to be a top-five risk overall, only 34% of organizations allocate more than 5% of their audit effort and 6% more than 10% of effort towards this. Our 2024 survey revealed a similar mismatch, with a #3 risk ranking yet #12 ranking in level of effort.

Talent's interconnectedness with other risks has become more well-understood in recent years. **Boards and business leaders increasingly comprehend how talent risk can impact their ability to achieve their objectives of creating and protecting value for stakeholders**. While it has always been clear how talent risk can compound operational, financial, and reputational risks, they now see how the ability to access specialized skill sets and different perspectives is essential to innovation and competitive differentiation and how increased use of third parties to support core operations can cause third-party, digital, and culture risks to swell. Internal audit should assess whether management understands this interconnectedness and is addressing talent in a way that ensures organizational objectives will be supported by talent, not hindered.

Low-Rated Risks With Comparatively High Audit Effort

Fraud: #10 Risk/#3 Audit Effort

A large majority (71%) of internal audit functions continue to allocate more than 5% of their time to this lower-ranking risk. Sadly, this finding reflects a longstanding trend of mismatched effort-to-risk in the area of fraud.

Granted, internal audit historically has been tapped to cover fraud; it's an area in which most of us are experienced and comfortable auditing. **But is it truly the best place to invest our already limited time and resources?** What's more, the bulk of the effort expended toward preventing or quickly addressing fraud should ideally be a first- and second-line responsibility.

ESG: #13 Risk/#9 Audit Effort

About half of the CAEs surveyed say they dedicate more than 5% of their total audit effort to ESG risk, even while acknowledging that it isn't a priority. To be clear, I do not want to discourage audit coverage of this vitally important risk. **The real question we should be asking: Why is ESG risk rated so low?** Organizations may need to revisit ESG's lack of prioritization in their overall risk strategy. Further, they may need to determine where ESG risk is "hiding" insofar as it is being recognized as such when audit effort is allocated.

“Matches” That Deserve a Second Look

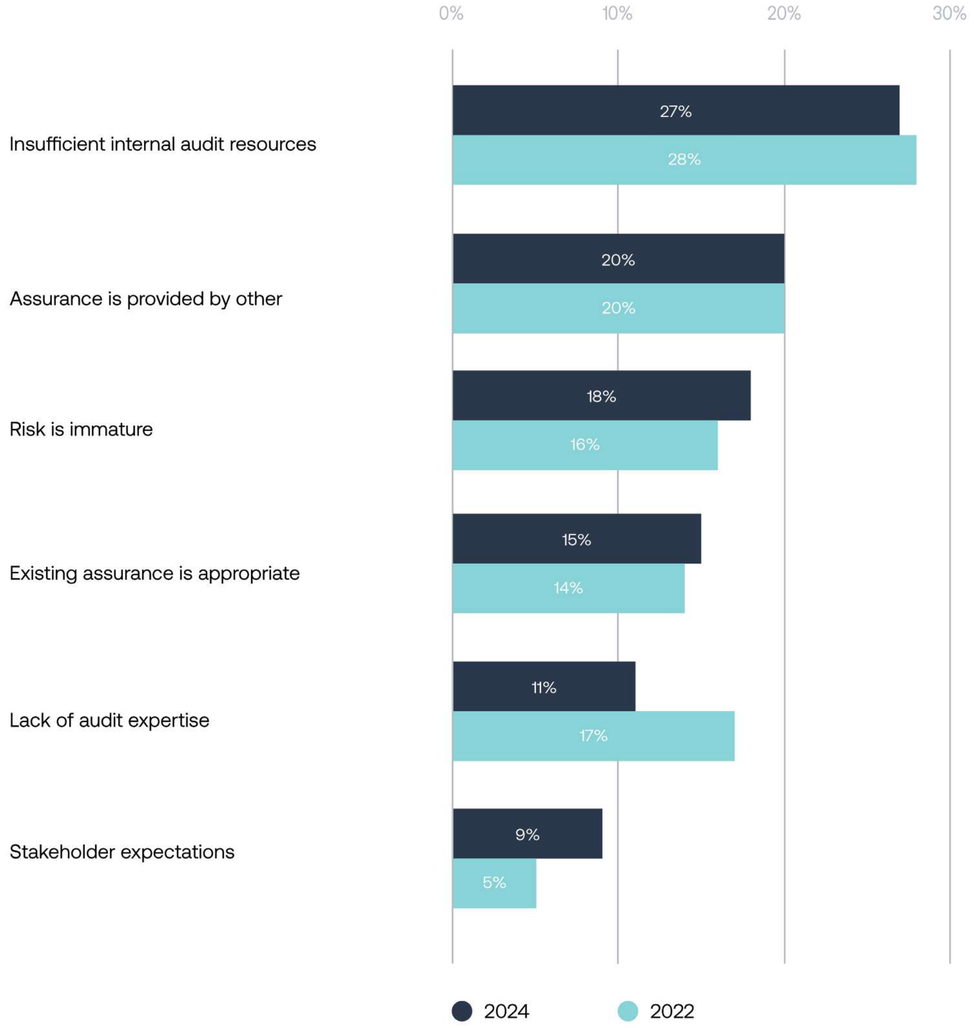
The survey revealed two key areas in which risk and effort levels ostensibly match, but which in fact warrant closer examination. In these cases, internal audit’s perception of risk often seems off-target and many CAEs would be well-served to invest more focus and effort. Specifically:

- **Organizational culture shouldn’t be both low risk and low effort.** As mentioned, this risk is too often overlooked or underestimated — until it explodes. While culture can be addressed in virtually any audit, it is essential that internal auditors recognize the risk overall and ensure that it is more fully assessed.
- **AI risk shouldn’t be both low risk and low effort.** This critical and fast-expanding risk area deserves our immediate focus. As I outlined in a 2024 blog, AI presents urgent risks that internal auditors cannot afford to ignore, in terms of its accuracy and accountability, ethical considerations, data privacy issues, talent disruption, governance, regulation, and intellectual property and legal vulnerabilities.

Understanding the Reasons for the Mismatch

Given the sustained trend of mismatched risk levels and audit efforts, the *2025 Focus on the Future* survey sought to understand the reasons behind it. **How do internal audit leaders see — and explain — these apparent mismatches?** Figure 11 compares our 2025 survey responses with those we received the last time we asked the question, in our 2023 survey (reflecting 2022 figures).

(FIGURE 11) *Explanations for Risk/Effort Mismatch*



Honing in on the more potentially questionable responses:

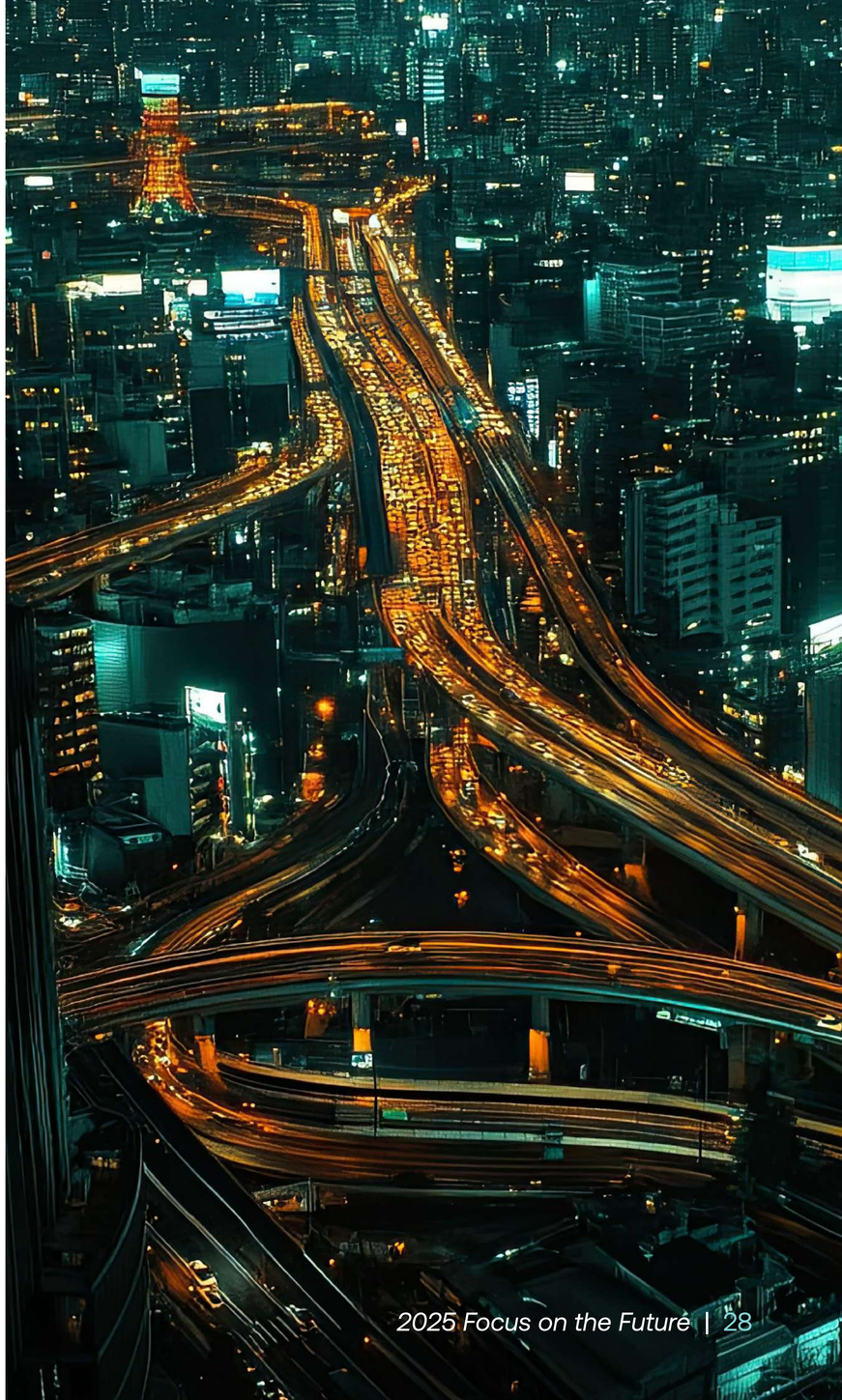
- **Insufficient resources.** This isn't a great reason, because **whatever your headcount, allocation should be based on risk**. We may feel like we don't have "enough" resources, but the data consistently shows that we're not always using them in the right ways (e.g., too much time spent on fraud). We must make sure the important things get done, even if they happen to be in challenging areas where we lack expertise (e.g., AI). In these cases, as appropriate, we should acquire the needed expertise internally or source it externally.
- **Lack of expertise to fully address the risk topic.** This is the only response that moved significantly between 2022 and 2025, decreasing by six percentage points. **Have we lulled ourselves into thinking we know "enough" about our key risks?**
- **A risk is not yet mature enough for internal audit's attention.** Again, I question the validity of this response when so many internal auditors seem to be underestimating AI risk. **A risk does not have to be mature to have a massive impact on your organization.** Auditors must be willing to address risk as its effects are emerging and forming — and not wait until the damage has been done.

The responses reveal a few noteworthy trends:

- Not surprisingly, **smaller internal audit departments** are more likely to cite insufficient resources and/or "stakeholder expectation is for less attention to the risk." Indeed, when resources are in short supply, internal auditors are unlikely to do more than what stakeholders are asking for.
- **Government and education organizations** are more likely to cite insufficient resources — and the least likely to say that existing assurance is appropriate.
- **Larger audit functions** are more likely to say that existing assurance is appropriate. This makes sense, given that larger functions can often increase efficiency in ways that reduce the level of audit effort.

KEY QUESTION

Some of these explanations are understandable. But others beg the question: **Are risks genuinely not changing? Or are some of these CAEs simply creatures of habit, and not altering where they spend their time from year to year?**



As we've shown, many of today's most daunting risks are indeed staying put at the top of organizations' collective risk rankings. The top five have been remarkably sticky in recent years, with the lower four jockeying for position below the sovereign "cybersecurity and data security." **But organizations have far more than five risks — and I worry that the remaining risks aren't always being assessed and managed in a manner befitting actual risk levels.** This worry is reinforced by the ongoing mismatches between risk rank and level of audit effort, as well as the low rankings of pressing risks such as AI, organizational culture, and ESG.

To effectively address the emerging and evolving threats and opportunities of permacrisis, organizations must be ready to adapt to changing conditions. While surveys can reveal only so much about what's really happening, *2025 Focus on the Future* does not suggest that internal auditors are consistently following the risks and flexing audit plans and risk management in real time.

If we're truly going to be the risk-centered profession we profess to be, we should not see so many anomalies in which the risk is so much greater than the audit focus — or the audit focus is so much greater than the risk. **Internal auditors should take pains to clearly understand if and why these mismatches have occurred in their organizations, and whether they are acceptable for effective risk management.**

Future-Focused Auditor Tip

Risk management should be integrated throughout the organization and aligned with strategy and performance. These key tenets underpin both the COSO ERM Framework and ISO 31000 Risk Management Guidelines, supporting organizations in:

- Integrating **risk-based decision-making** into the organization's resource allocation, governance, management, planning, reporting, policies, values, and culture.
- Understanding **risk in the context of performance**, rather than as an isolated exercise.
- More clearly connecting risk management with **stakeholder expectations**.
- Assigning **responsibility and accountability** at appropriate levels throughout the organization, and **creating a risk-aware culture** in which employees and stakeholders understand the importance of effective risk management and monitoring.
- Understanding how risks affect the **relevance and viability of the organization's overall strategy**, as well as the risk implications from the chosen strategy.

Resources and Talent: Risk Grows While Resources Stagnate

Make no mistake: Risk volume and complexity are increasing. *The State of Risk Oversight*, a 2024 global report from the American Institute of Certified Public Accountants (AICPA), Chartered Institute of Management Accountants (CIMA), and NC State University, found that 65% of all executives (70% from large organizations) believe their organizations' risk volume and complexity have "mostly" or "extensively" increased in the past five years. **In turn, risk teams' responsibilities are expanding**: KPMG's *2024 Future of Risk* report found that 61% of surveyed executives expect to see a significant increase in the level of risk they will be responsible for in the next three to five years.

As risk mounts and changes, CAEs strive to allocate the right resources to the right areas. It's a continual balancing act in which big goals and "best-laid plans" often fall victim to budget pressures and changing priorities. CAEs must nonetheless strive for a realistic outlook, avoiding surprises and shortfalls down the road. Unfortunately — continuing another recent Focus on the Future trend — **2025's survey reveals a pattern of ongoing budget and staffing optimism at odds with continuing macroeconomic uncertainty and a fluctuating labor market.**

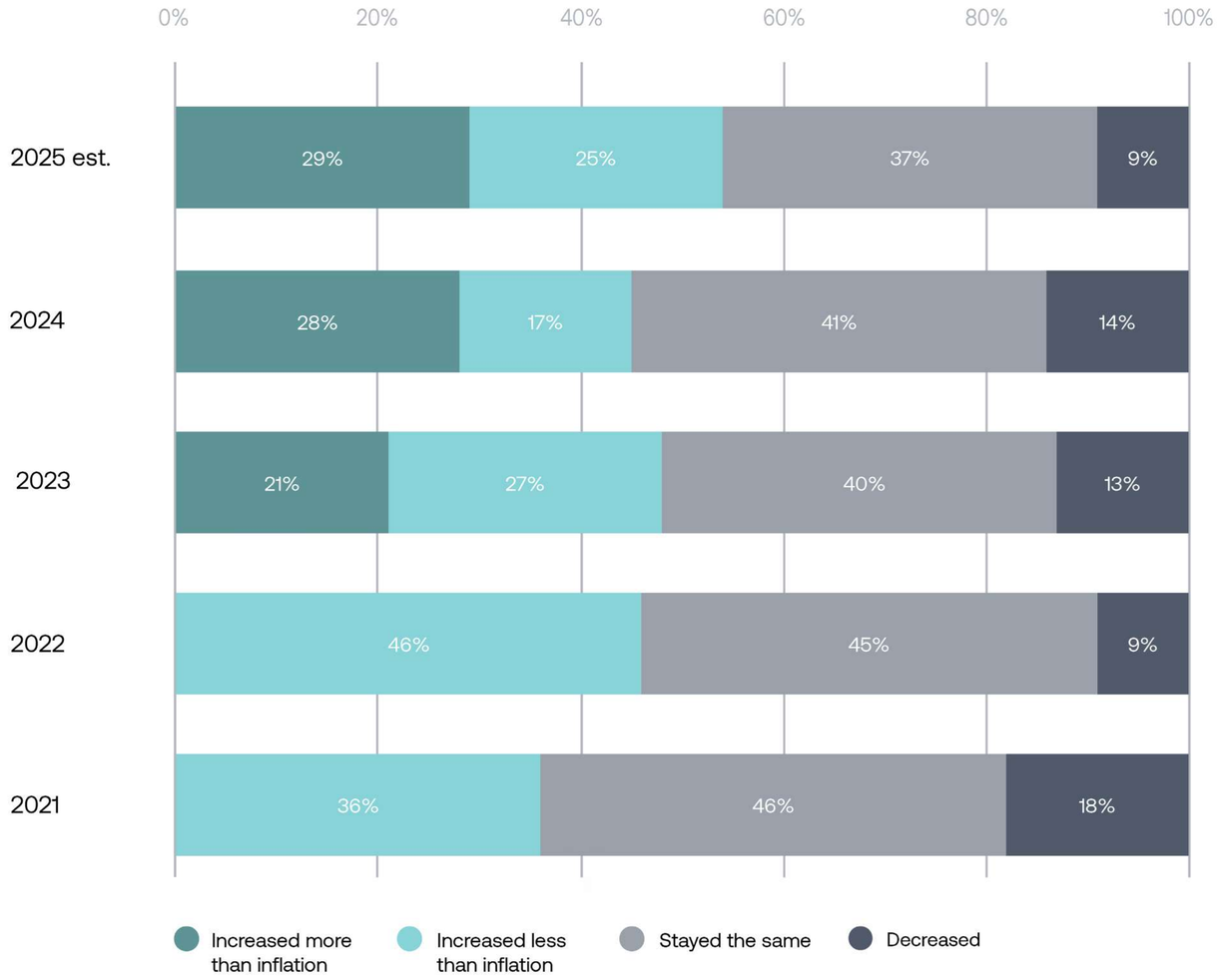
Internal Audit Budget Outlook

More than half (54%) of internal audit leaders anticipate that their budgets will increase in 2025. Generally speaking, the highest percentage increases are expected by smaller audit departments, with larger audit departments anticipating lower percentage increases. As Figure 12 illustrates, only 9% of respondents expect budget decreases in 2025.

Unfortunately, history shows that budget expectations rarely align with budget realities. More than 60% of last year's survey respondents expected budget increases in 2024. Though the respondent pool obviously varies from year to year, it remains notable that only 45% of survey respondents report actual increases in 2024. Similarly, 9% of respondents last year predicted 2024 budget decreases, while 14% now report actual 2024 decreases.

We can and should celebrate the growth of internal audit departments whose budgets are increasing faster than inflation, but in reality this group is a minority. **The data paints an overall picture of a profession that is largely stagnant.** Budget growth is tepid at best, especially when viewed in the context of permacrisis' ever-increasing risk volume, velocity, and volatility.

(FIGURE 12) *Internal Audit Budgets, 2021–2025*



Internal Audit Staffing Outlook

While more than half of respondents forecast budget increases in 2025, an overwhelming number see their headcounts going unchanged. Specifically, 67% anticipate their headcount will stay the same, 26% foresee an increase, and only 7% expect a decrease. Fortunately, as shown in Figure 13, respondents' 2025 forecasts largely resemble their reported 2024 actuals — however, only 6% of 2024 survey respondents anticipated staffing decreases, and 11% of 2025 survey respondents report actual decreases in 2024.

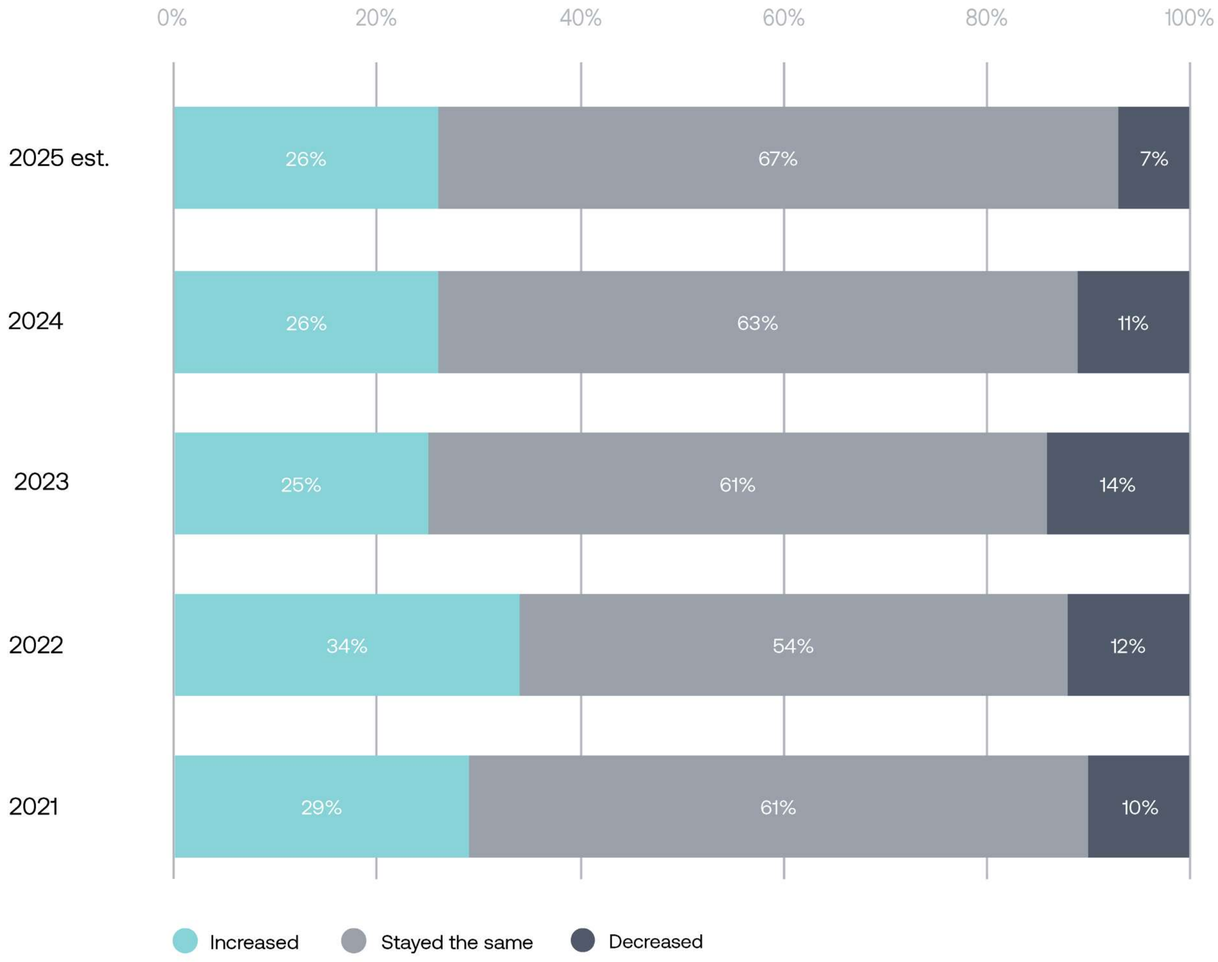
AuditBoard survey data from the past three years collectively reveal a clear pattern of optimistic staffing forecasts followed by less rosy realities. **CAEs consistently forecast lower headcount decreases than actually occur, such that only half who had decreases saw them coming.** They also tend to predict higher headcount increases than actually occur.

In other words, whatever your expectations, history shows that you're unlikely to fully realize them. **After all, volatility and uncertainty are among permacrisis' only constants.**

KEY QUESTION

Why do internal auditors largely continue to anticipate receiving more resources than expected? Rarely do unforeseen risks result in internal audit departments receiving more resources than expected. That hasn't happened since the Sarbanes-Oxley Act of 2002 (SOX).

(FIGURE 13) *Internal Audit Headcounts, 2021–2025*

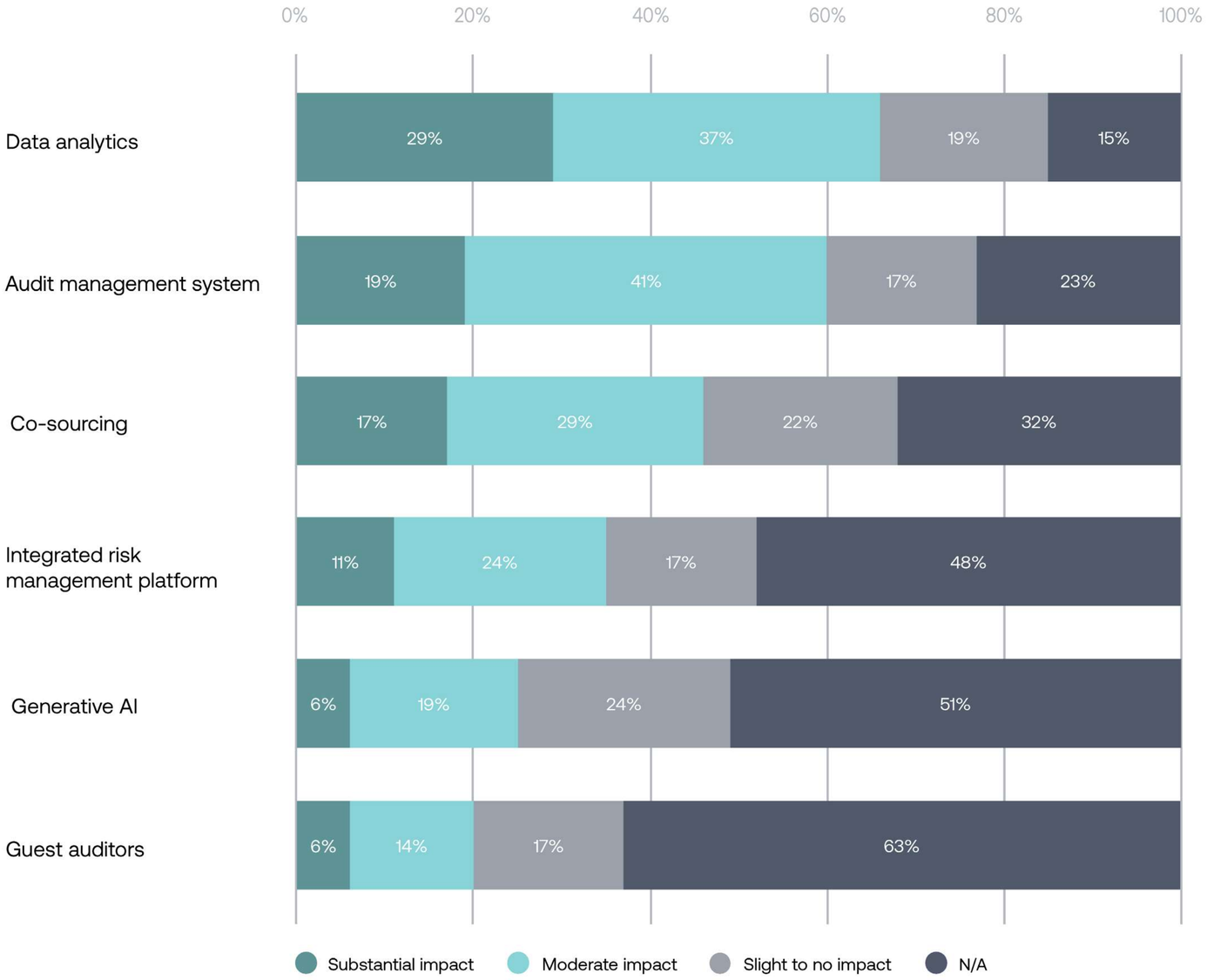


Impact of Capacity Multipliers

Internal audit teams facing resource constraints need to find innovative ways to do more with less. That often means implementing capacity multipliers, which are initiatives focused on improving efficiency to produce more output from limited resources. Our 2025 survey sought to identify which strategies are having the greatest impact by asking CAEs to look back at efforts over the past two years.

Internal audit teams are finding at least moderate success with several strategies, as reflected in Figure 14. Unfortunately, survey results also indicate that most functions rely primarily on capacity multipliers that have been used for decades, missing out on key opportunities from newer approaches.

(FIGURE 14) *Impact of Capacity Multipliers*



The IAF's *Vision 2035* report also explored the use and impact of capacity-multiplying technology tools and approaches, asking internal auditors to assess which are most important for the future of internal audit. To expand our view on this vital topic, we compared our *2025 Focus on the Future* survey results with relevant *Vision 2035* findings.

- **Tried-and-true capacity multipliers are most often used and viewed as impactful.** Most respondents use data analytics (85%) and audit management systems (77%).
  - **Data analytics are seen to have the greatest impact**, viewed by 66% as having a substantial or moderate impact.
  - **Audit management systems rank second for impact**, assessed by 60% as having a substantial or moderate impact.
- **Adoption of newer capacity multipliers is lagging in many internal audit functions.**
  - Approximately half or more of respondents are not using integrated risk management (IRM) software or generative AI.
  - **Most notably, 51% have not implemented AI, and only 25% assess it to have a noticeable impact.**
- **Staffing-oriented approaches receive mixed feedback.**
  - **Most respondents do not see guest auditors as impactful.** A mere 20% judge them to have a significant impact, and a surprising 63% don't even use them.
  - **Co-sourcing was implemented by most departments (68%), but a worrying 22% say the efforts have little to no impact.**

← This aligns with *Vision 2035*'s findings: 91% of respondents assess data analytics as being most important for internal audit's future.

← 75% of *Vision 2035* respondents view audit management systems as being most important for internal audit's future.

← *Vision 2035* also finds low levels of implementation, with 77% reporting low or no implementation of AI. At the same time, **74% see AI as being most important for internal audit's future**.

KEY QUESTIONS

Why aren't audit management systems considered more impactful? Are they simply viewed as "table stakes" — a standard component of our work, taken for granted? Alternatively, do these results reflect a failure to properly implement the full range of these systems' potential capabilities? **Lastly, why are nearly a quarter of respondents still not using them?**

Why aren't more internal auditors implementing AI? Its potential as a capacity multiplier grows daily, and as Vision 2035 reinforces, most know AI is critical for supporting an ideal future for internal audit. Still, high levels of AI implementation appear to be rare: Vision 2035 finds that only 7% of respondents have implemented AI at an advanced or high level.

Are you doing enough to drive the most benefit from your analytics? Analytics have been around for decades, so they are also seen as table stakes to a degree. As Vision 2035 asserts, however, **the challenge now is to** advance how we use analytics: The "internal auditor of the future" uses "advanced analytics to provide robust, evidence-based assurance and forecast future organizational trends with unprecedented precision."

There's an old excuse about being "too busy to plan." That could be internal audit's tagline, as so many departments say they feel too busy to innovate. Certainly, it takes time, energy, and courage to lean into new technologies. Further, if no one is pushing us, it's easier to stay the course. This may help explain the lagging adoption and use. But as *Vision 2035*'s findings reinforce, regardless of what internal auditors are *doing* in 2025, they are clear-eyed about what's needed to ensure our ideal future. Why would we ignore our own predictions? **We can't afford to pass up the opportunities we ourselves identify as central to our future.**

Future-Focused Auditor Tip

Embed capacity multipliers as part of your strategic audit plan. "Innovate to add more value" is one of *Vision 2035*'s central calls to action, essential for safeguarding and enhancing stakeholder value. The internal audit profession is still not making the most of its available capacity multipliers — especially those enabled by technology. Make sure your strategic plan explicitly addresses how you will explore, implement, and optimize specific capacity multipliers (e.g., AI, advanced analytics) within set time frames.

Internal Audit at Mid-Decade: An Inflection Point

The first half of the 2020s offered internal auditors an invaluable opportunity to redefine who we are and what we do. As our organizations continue to be disrupted, tested, and reshaped by permacrisis, leaders need internal audit's objectivity, independent assurance, business acumen, and cross-organizational risk expertise more than ever.

I have no doubt that many internal auditors have embraced this opportunity to step up as trusted advisors and agents of change, delivering the insight and foresight their organizations need to navigate the road ahead. Unfortunately, **many internal auditors still have made only tepid progress toward transformation**. This is a key strategic risk threatening our future.

We stand at an important crossroads. *Connected Risk: Conquering the Perilous Risk Exposure Gap* imagines three possible futures: (1) Complacency causes us to nose-dive, (2) we stay the course and glide by, or (3) we seize the opportunities and soar. You all know my vote.

Picture the journey ahead as a mountain that the internal audit profession must scale. Many internal auditors are taking the slow and steady route, plodding diligently up the switchbacks. While they may make it to the top eventually, such slow progress is not enough. The current risk landscape demands more. The need now is to gather the right tools, summon courage, band together, and proceed straight up the mountainside. This requires approaching our work in new and different ways, and reimagining our roles to better meet our organizations' needs in the modern age.

A Future-Focused Checklist for 2025 and Beyond

- [ ] **Cultivate a strategic internal audit culture.** Set clear expectations that complacency is not a strategy and innovation, collaboration, and transformation are vital. We can't get where we need to go without making flexible, risk-informed plans to get there. By working together to agree on a destination, anticipate potential pitfalls, start on a path, and pivot as needed, we greatly increase the chances of reaching our desired destination.

- [ ] **Embrace risk and uncertainty with skill and confidence.** A climate of uncertainty is an opportunity for internal audit to shine. Business leaders and boards increasingly understand just how much they don't know. Internal audit's insight and foresight can play a pivotal role in helping organizations become more effective in identifying, monitoring, and mitigating both existing and emerging risks.

- [ ] **Become beacons of insight and foresight through advisory services.** As analytics, AI, and centralized governance, risk, and compliance technologies enable us to do more with less, time and resources are freed up to deliver more value through advisory work. Does your organization truly need another fraud audit — an exercise in hindsight? Or does it need strategic, risk-based insights on the threats and opportunities that could impact performance and resilience?

- [ ] **Overcome hesitations to embrace AI and other enabling technologies.** AI is here to stay. If we prove ineffective in using AI to augment our skills, we increase the risk that our organizations may start seeing AI as a means to supplant those skills.

- [ ] **Abandon silos, moving from three distinct lines to a connected risk approach.** As the new Standards reinforce, "collaborating" is not "conspiring." Internal auditors can collaborate with first- and second-line colleagues without compromising their objectivity or independence. A connected risk model respects each team's distinct purpose and value while connecting and aligning them around the shared objectives of value protection, creation, and realization. Connected risk creates a whole greater than the sum of its parts — a powerful path forward for effective risk management amid permacrisis.

Methodology and Participants

Methodology

AuditBoard developed a custom online questionnaire to survey 376 internal audit professionals. These individuals represent enterprise organizations across varying industries in the United States, United Kingdom, and Ireland. All survey participants were in directorial roles or above. The survey was fielded between August 8, 2024 and August 20, 2024.

Participants

N = 376 global internal audit professionals

Primary Industry

FINANCE AND INSURANCE	27%
SERVICES	21%
INDUSTRIAL	26%
GOVERNMENT AND EDUCATION	17%
TECHNOLOGY	9%

Annual Revenue

<$250M	16%
$250M - $1B	19%
$1B - $2.5B	17%
$2.5B -$10B	22%
$10B +	14%
I DON'T KNOW/CANNOT DISCLOSE	12%

Company Holding

PUBLICLY-TRADED FOR PROFIT	43%
PRIVATELY HELD FOR PROFIT	29%
NOT-FOR-PROFIT	8%
PUBLIC SECTOR	20%

Approximately how many FTE auditors are in your organization?

1–2	12%
3-6	33%
7-15	23%
16-30	14%
MORE THAN 30	18%

About the Author

RICHARD CHAMBERS
Senior Internal Audit Advisor
AuditBoard

Richard Chambers is the CEO of Richard F. Chambers & Associates, a global advisory firm for internal audit professionals, and also serves as Senior Advisor, Risk and Audit at AuditBoard. Previously, he served for over a decade as the President and CEO of The Institute of Internal Auditors (The IIA), where he led the organization to record global membership and countless milestones. Prior to The IIA, Chambers was national practice leader in Internal Audit Advisory Services at PwC, Deputy Inspector General of the U.S. Postal Service, and Inspector General of the Tennessee Valley Authority.

About AuditBoard

AuditBoard is the leading cloud-based platform transforming audit, risk, compliance, and ESG management. More than 50% of the Fortune 500 leverage AuditBoard to move their businesses forward with greater clarity and agility. AuditBoard is top-rated by customers on G2, Capterra, and Gartner Peer Insights, and was recently ranked for the fifth year in a row as one of the fastest-growing technology companies in North America by Deloitte. To learn more, visit AuditBoard.com.