CAEs view cyber threats, talent management and third-party risks as top concerns

By Andrew Struthers-Kennedy

Boards of directors and senior executive teams face a complex web of uncertainties. These may generate opportunities for strategic advantage or risks leading to unexpected disruption and performance shortfalls. An ability to anticipate risks that may be on the horizon before they become imminent can help leaders navigate unfolding developments – particularly those that are uncontrollable – that may impact their organisation's value and growth objectives.

Our 13th annual **Executive Perspectives on Top Risks Survey** contains insights from 1,215 board members and C-suite executives around the world regarding their views on the top risks they see on the near- and long-term horizon. Specifically, our global respondent group provided their perspectives about the potential impact over the near-term (two to three years ahead) and long-term (over the next decade) of 32 risk issues across these three dimensions:

- **Macroeconomic risks** likely to affect their organisation's growth opportunities
- **Strategic risks** the organisation faces that may affect the validity of its strategy for pursuing growth opportunities
- **Operational risks** that might affect key operations of the organisation in executing its strategy

Commentary – perspectives of chief audit executives

In a dynamic business landscape filled with uncertainty, CAEs perceive most of the macroeconomic, strategic and operational risks organisations face to be higher magnitude threats compared to CEOs, CFOs and other C-suite respondents to our latest Top Risks Survey. This makes it imperative for internal audit leaders to work closely with leaders in the enterprise to ensure that risks are thoroughly understood and sufficiently addressed.

For CAEs, the top near-term risks globally (looking out two to three years) include cybersecurity, talent management, third-party risks, economic conditions and heightened regulatory scrutiny. Furthermore, internal audit leaders believe these same risk concerns will be significant challenges for their organisations over the next decade. We view that forecast positively in one respect: It suggests that investments today in talent, technology, innovation and transformation will better prepare internal audit groups, and the organisation as a whole, for future challenges.

Investments today in talent, technology, innovation and transformation will better prepare internal audit groups, and the organisation as a whole, for future challenges.

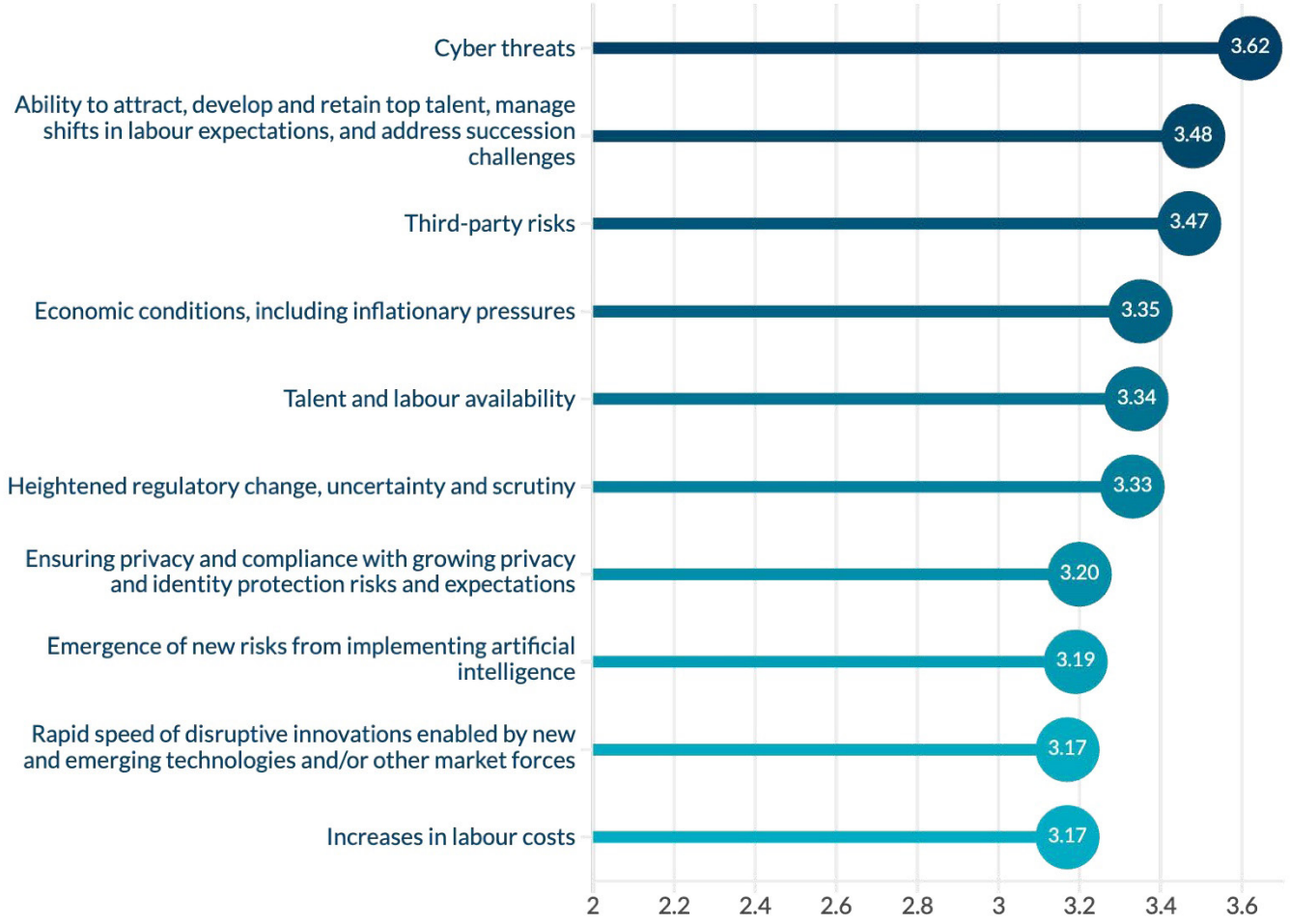
Also of note, three of these risks are operational in nature, which is to be expected given that, unlike some other executives, internal audit's focus tends to be on operational areas that the organisation can control and which are more readily auditable. Other highly rated near-term operational risk issues include privacy compliance and emerging risks from the use of artificial intelligence (AI). That said, it's important for internal audit leaders to not lose sight of key macroeconomic and strategic risk issues as well.

Overview of near-term top risks

For CAEs, the near-term risk outlook is focused squarely on cybersecurity, talent, third-party concerns, economic conditions, and regulatory change and challenges. Privacy and AI are also very much on the radar. Given CAEs' broad views of risks their organisations face and what is commonly a sceptical and typically risk-averse nature, it is perhaps no surprise that they rated risks at higher levels of significance than any other C-suite or board respondents, though chief risk officers and board members are not far behind in their views in terms of perceived levels of risk impact. For internal audit leaders, this also is a function of the deeper level of insights they have with respect to the true level of residual risk for the organisation, the effectiveness of mitigation activities, and management's understanding of and readiness to respond to risks.

The chart on the following page displays the top 10 near-term risks for CAEs and is followed by our perspectives on the higher-rated risks and some broader themes.

CAEs – near-term outlook



Cyber threats

Cybersecurity threats top the list of CAE risk concerns in the near-term outlook. Further, in line with their risk-and-control mindset, internal audit leaders rate cyber threats at a significantly higher risk level than do their C-suite colleagues. These findings are consistent with related research conducted by Protiviti and The Institute of Internal Auditors (The IIA) that identifies cybersecurity as the top technology risk CAEs and technology audit leaders confront. Of note, this joint research shows that internal audit teams which perform more frequent, technologically advanced audits are more likely to perceive cybersecurity as a high-magnitude threat.

Beyond factors such as the ever-evolving threat landscape and potential severity of the consequences of an attack or sensitive data breach, CAE views on cyber threats are being driven by a number of factors, including:

1. **Ongoing cyber oversight** – Internal audit groups are assessing cyber risks with greater frequency and sophistication (e.g., using AI to enhance technology audits). Threat actors are continuing to evolve their capabilities. In response, management needs to increase their controls, capabilities

and tooling so that internal audit teams have full visibility and can help evaluate management's efforts to manage cyber risk.

2. **Internal audit's mandate** – Assessment of cybersecurity risks is a key part of internal audit's risk and oversight focus and responsibilities, combined with its duty to protect organisational value. Of note, The IIA recently issued a Topical Requirement on cybersecurity. This guidance provides a consistent, comprehensive approach to assessing the design and implementation of cybersecurity governance, risk management and control processes. The requirements represent a minimum baseline for assessing cybersecurity in an organisation.[1]
3. **Growing regulatory requirements** – There are an increasing number of regulatory requirements worldwide concerning cybersecurity capabilities and required disclosures. For example, in addition to the U.S. Securities and Exchange Commission's (SEC's) cybersecurity disclosure rules, organisations now must comply with the European Union's (EU's) Network and Information Security Directive 2 (NIS2), which expands the scope of the original directive unifying national laws with common minimum requirements designed to further enhance cybersecurity throughout the EU.

In response to intensifying bad-actor threats and cyber-related compliance demands, internal audit groups are scrutinising organisational defences against data breaches, ransomware, increasingly sophisticated social engineering attacks (many of which are now being enabled through AI technologies), third-party and supply chain risks, and cloud service provider security vulnerabilities. These cybersecurity areas of focus help explain why CAEs also rate third-party risks as a significant near-term concern.

As CAEs consider their talent strategies, they should continue to evaluate their options to gain access to the necessary skills and knowledge to allow them to conduct an increasingly broad range of often technical cyber-related reviews.

In addition to "core" cybersecurity program reviews to evaluate cyber preparedness and address these cyber-related topics, CAEs and internal audit functions should continue partnering with management to assess other cyber-adjacent areas, including but not limited to data privacy and compliance, data governance and integrity, adoption of AI technologies, technical debt and aging infrastructure (and related technology modernisation efforts), third-party security controls, integrated cyber risk reporting frameworks, and data classification schemes.

Lastly, as CAEs consider their talent strategies, they should continue to evaluate their options to gain access to the necessary skills and knowledge to allow them to conduct an increasingly broad range of often technical cyber-related reviews.

[1] *Cybersecurity Topical Requirement*, The Institute of Internal Auditors, February 2025: www.theiia.org/globalassets/site/standards/topical-requirements/cybersecurity/cybersecurity_topical_requirement.pdf.

Talent availability and management

Mirroring concerns expressed by most board members and C-suite leaders, talent remains a pressing risk issue for CAEs and many view this from two dimensions: the talent needs and challenges specific to their own departments and the talent-related risks faced by the broader organisation. CAEs are concerned about the organisation's and their own function's ability to attract, develop and retain top talent which, as an operational risk, can be controlled to a large degree by the organisation. Broader risks related to talent availability and labour costs are largely out of the organisation's control, but they need to flex and adapt to these external conditions and dynamics, particularly where there are significant talent pipeline challenges. Such issues already are emerging in finance and accounting.[2]

Talent remains a pressing risk issue for CAEs and many view this from two dimensions: the talent needs and challenges specific to their own departments and the talent-related risks faced by the broader organisation.

Sustaining access to top talent, and top technology talent in particular, is of growing importance. This challenge directly affects CAEs, who are hard-pressed to recruit, develop and retain the skills they need to execute increasingly technology-focused and technical audits while also advancing the internal audit function's own digital transformation. Further, they require qualified and experienced professionals to support core audit and advisory activities related to organisation-wide technology initiatives such as AI implementation and broader technology modernisation efforts.

In light of CAEs' concerns about cybersecurity, third-party risks, marketplace disruptions and risks that arise from AI implementations, technology talent management – from recruiting pipelines to retention programs – should be addressed as part of internal audit strategic planning and articulated clearly in the internal audit strategic plan (now a requirement in The IIA Standards, specifically Standard 9.2). It also should be addressed in communications with executive stakeholders and the audit committee. Access to skills in AI and other emerging technologies (in-house or via external partners) directly affects the company's ability to capitalise on, as well as effectively risk-manage and govern, these technologies to maintain or grow its competitive edge as well as to manage related risks. CAEs should consider whether foundational technology knowledge and acumen represent a base-level required skill for all team members. There are strong arguments for creating an upskilling program for the internal audit function that develops a level of competence in these areas at least at the "minor" level, to complement the "major" for the individual.

Third-party risks

CAEs understand the inherent risks and challenges posed by what for many is an increasingly complex and multidimensional third-party ecosystem. There have been numerous instances of business

[2] "Navigating the Accounting Pipeline Crisis," Anthony J. Tucci, LLM, JD, CPA, The CPA Journal, February 2025: www.cpajournal.com/2025/02/14/navigating-the-accounting-pipeline-crisis/.

disruption, of various kinds, that have been tracked back to issues at a third party. As organisations have increasingly integrated with and relied upon third parties for technology solutions, operational support and other critical facets of their business activities, the need for robust third-party risk management programs, along with independent auditing of these programs and the risk management and control processes of third parties, has never been more critical.

Robust coordination and collaboration with teams responsible for overseeing and managing third-party risk is critical and speaks to the broader need for CAEs to be engaging with counterparts overseeing other risk and assurance teams within their organisations.

CAEs must ensure they have a current, comprehensive view of third-party relationships and management's approach to managing risks associated with these third parties (including consideration of fourth parties) in areas including data sharing and systems access, security and privacy, contracting, regulatory compliance, performance obligations, assurance reporting, and more. This is an area where robust coordination and collaboration with teams responsible for overseeing and managing third-party risk (e.g., information security, business continuity, procurement, supply chain) is critical and speaks to the broader need for CAEs to be engaging with counterparts overseeing other risk and assurance teams within their organisations.

The economy

Economic conditions, including inflationary pressures, rate as a top CAE risk concern amid heightened global uncertainty stemming from changes to trade and financial policies in the United States as well as other countries, geopolitical flashpoints, natural disasters, and other macroeconomic factors. While macroeconomic factors may not be directly auditable, the ways in which an organisation plans for and reacts to a range of potential and likely scenarios, as well as underlying operational processes – such as supply chain resilience, organisational agility, change readiness and disruption response – should be squarely on the list of risks that are subject to periodic assessment and audit planning consideration.

With respect to the potential for significant downward trends in economic conditions, internal audit is in a position to assess the organisation's "down economy playbook" and determine how it will be able to manage through reductions in spending, workforce disruption (including the impact to risk management and control processes thereof), and other impacts brought about by a decline in business conditions, while also performing audit and advisory reviews over business enablers such as technology modernisation strategies and programs and AI adoption and enablement. Such initiatives can help unlock additional capacity and drive significant increases in operational efficiency and effectiveness.

Overview of top risk issues for 2035

CAEs' longer-term concerns largely mirror their near-term risk priorities, with several subtle differences. When asked to identify two concerns from each risk category in the survey (macroeconomic, strategic and operational) they expect to pose the greatest challenges to their organisations over the next decade, internal audit leaders most frequently identified:

- Economic conditions and talent availability (macroeconomic)
- Regulatory change and the rapid speed of disruptive innovations (strategic)
- Cybersecurity and third-party risks (operational)

Each of these six long-term risk concerns also rate among the top 10 near-term risk concerns for CAEs.

CAEs – long-term outlook

Macroeconomic risk issues

Risk	Percentage
Economic conditions, including inflationary pressures	43%
Talent and labour availability	38%
Geopolitical shifts, regional conflicts and instability in governmental regimes	25%

Strategic risk issues

Risk	Percentage
Heightened regulatory change, uncertainty and scrutiny	40%
Rapid speed of disruptive innovations enabled by new and emerging technologies and/or other market forces	32%
Sustaining customer loyalty and retention	24%

Operational risk issues

Risk	Percentage
Cyber threats	38%
Third-party risks	31%
Ability to attract, develop and retain top talent, manage shifts in labour expectations, and address succession challenges	25%

Note: Respondents were asked to identify the "top two" risks in each category (macroeconomic, strategic, operational) separately. That is, respondents identified six risks (two in each category) as "top two" risks. For each category, the three risk issues receiving the most responses by percentage are shown.

This continuity suggests that CAEs expect the threat magnitude of these risks to sustain or intensify over the next 10 years, and perhaps also points to the inherent challenges in thinking through and forecasting risks over a long-term time horizon. Economic uncertainty in many major global economies remains, with a continued lack of consensus about near- and longer-term economic forecasts. Business and broader economic conditions tend to influence areas of focus heavily, along with the pace and nature of operational spend and capital investment. There remain concerns that talent and

labour supplies will remain constrained, particularly in areas of evolving demand that will require robust strategies related to hiring, upskilling and re-skilling, leveraging third parties for both surge needs as well as subject-matter expertise, and other ways in which organisations can gain access to necessary talent.

Global regulators – at the national and sub-national levels – will continue to enact new requirements and amend or rollback existing regulations. Being prepared and able to respond to rapid changes in the regulatory landscape will be key to helping ensure efficient and effective regulatory compliance programs.

New technologies will continue to emerge and be adopted and will have wide-ranging impacts, from competitive differentiation and customer retention to adoption risk, talent, cyber and more. And ongoing cyber threats and third-party risks will continue to pose challenges on multiple fronts.

Call to action for CAEs and internal audit leaders

Talent and technology are running themes on the list of top risks for CAEs. Apart from uncertain economic conditions, each of the CAE's top five risk concerns relate to technology (cybersecurity and third-party risks) or talent management (the organisation's ability to attract, develop and retain top talent as well as the availability of that talent). To address these risks, audit leaders must perform a variety of enabling actions. This work involves:

C-suite alignment – The risk concerns of CAEs differ from those of their C-suite colleagues, for both the near- and long-term views, in two ways. First, as we have mentioned, internal audit leaders generally rate most risks to be more significant than do their executive counterparts. Secondly, they prioritise their risk concerns differently. Both of these points are worthy of discussion, constructive challenge, and reconciliation or alignment. Understanding what is influencing the perspectives (on ratings and rankings) is important and constructive dialogue. CAEs and their CRO counterparts are trained in, experienced in and tasked with identifying, assessing, escalating and reporting risk in ways that other executives simply are not. They bring a complementary skillset and point of view to that of other executives. Often inherent in that are increased levels of professional scepticism and risk aversion. This underscores the importance of CAEs maintaining clear, effective and ongoing dialogue with their C-suite colleagues and the board.

The geopolitical, environmental and technological flashpoints roiling global markets require organisations to muster more flexibility, agility and resilience than ever before.

A heightened focus on less "auditable" areas – The geopolitical, environmental and technological flashpoints roiling global markets require organisations to muster more flexibility, agility and resilience than ever before. Volatile economic conditions and risks are difficult to audit due to their fluid nature. The same holds true for enterprise resilience, agility and adaptability, all of which cut across business functions and must evolve continually. Long-term, CAEs need to consider new ways to audit these

complex risks, or at least the underlying organisational processes (whether those related to strategy or operations) to help identify and report gaps.

Cybersecurity and technology modernisation – CAEs' top risk concerns reveal issues that are both directly (e.g., cybersecurity, AI implementations, technology-driven disruptions) and indirectly related to technology advancements. Talent-related risks and rising labour costs are driven largely by intense competition for rapidly evolving technology skills. Third-party risks (e.g., data privacy and security) and regulatory risks (e.g., cybersecurity disclosure and AI governance requirements) are also driven in great part by technology advancements. These issues underscore the need for CAEs to sustain access to top technology talent and specifically to recruit, develop and retain the skills they need to execute technology-focused and technical audits and also advance the internal audit function's own digital transformation.

Talent-related risks and rising labour costs are driven largely by intense competition for rapidly evolving technology skills.

AI – CAEs should remind themselves that AI adoption represents the topmost risk concern for CEOs. In addition to addressing new AI-related risks – by monitoring its adoption, use and evolution throughout the organisation, as well as the governance frameworks that are put in place – internal audit groups should look to "supercharge" their teams through AI training and enablement, and embrace AI adoption to support internal audit activities across the entire internal audit lifecycle.

Talent – In addition to auditing the organisation's talent management strategies and plans, CAEs should assess and address talent and skills gaps in their own realm. Within internal audit departments, the need for AI, technology, cybersecurity, data governance, data analytics and third-party risk management proficiency continues to soar, yet CAEs must not overlook the need to invest in the development of skills that will create well-rounded and broadly capable internal auditors. Specifically, they must support the development of skills including creative thinking, critical thinking, effective communication, problem-solving, innovative thinking and more.

Your internal audit function for the future – Beyond the current frenzy around AI, CAEs must commit to a function that is technology- and data-enabled. CAEs should challenge themselves and their teams to answer questions such as "What is our ideal state with respect to the technology and data enablement of our internal audit activities?" and "What specific and complement of skills does my internal audit function of the future need to have?" Being thoughtful in contemplating these questions and then developing specific plans to address identified gaps will set CAEs on a path toward having a future-ready internal audit team.

About the Executive Perspectives on Top Risks Survey

We surveyed 1,215 board members and executives across a number of industries and from around the globe, asking them to assess the impact of 32 unique risks on their organisation over the next two to three years and over the next decade, into 2035. Our survey was conducted online from mid-November 2024 through mid-December 2024. For the near-term outlook, each respondent was asked to rate 32 individual risks on a five-point Likert scale, where 1 reflects "No Impact at All" and 5 reflects "Extensive Impact." For each of the 32 risks, we computed the average score reported by all respondents and rank-ordered the risks from highest to lowest impact.

We also asked executives to share their perspectives about long-term risks (over the next 10 years – 2035) by selecting the top two risks from each of the three dimensions (macroeconomic, strategic and operational). For each of the 32 risks, we calculated the percentage of respondents who included that risk as one of their two top risks for each dimension.

Read our *Executive Perspectives on Top Risks Survey* executive summary and full report at www.protiviti.com or http://erm.ncsu.edu.

About the author

Andrew Struthers-Kennedy is Protiviti's Global Leader of Internal Audit & Financial Advisory services. He is responsible for the strategy, offerings, consulting delivery and external alliance partnerships for all Protiviti's internal audit capabilities, including technology audit, audit innovation & transformation, strategy & technology enablement, and SOX and controls advisory services. With over 20 years of experience in internal audit, risk management and consulting, Andrew is inspired by and committed to leading a global team that pushes the boundaries for the profession by offering thinking, tooling, services and people that are truly best-in-class. His market focus is on increasing the relevance of and value delivered by internal audit, both in the boardroom and across the clients he serves.