CAEs forecast intense risk environment – cyber threats, talent shortages and technology disruptions loom large

by Andrew Struthers-Kennedy
Global Leader, Internal Audit and Financial Advisory, Protiviti

The combined analysis of risk insights from global executives for both 2024 and a decade out reveals several interrelated challenges that may result in significant events with the potential to test an organisation's business agility and resilience.

Changes in the profile of top risks from the prior year disclose a number of shifting conditions that may disrupt markets, including events triggered by intensifying geopolitical conditions. Many of those events are expected to have long-lasting impacts on business models and the competitive balance in a nuanced global marketplace. Board members and C-suite leaders who recognise these shifting realities and address them through robust, enterprisewide risk analyses that are aligned with business strategy possess a differentiating skill that positions their organisation's readiness and ability to adjust and pivot in the face of inevitable disruptive change as well as or better than their competitors.

In this 12th annual survey, Protiviti and NC State University's ERM Initiative report on the top risks currently on the minds of board members and executives worldwide. The results of this global survey reflect their views on the extent to which a broad collection of risks is likely to affect their organisations over the next year – 2024 – and a decade later – 2034. Our respondent group, which includes 1,143 board members and C-suite executives from around the world (among them, 193 CAEs), provided their perspectives about the potential impact over the next 12 months and next decade of 36 risk issues across these three dimensions:[1]

- **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

[1] Each respondent rated 36 individual risk issues using a 10-point scale, where a score of 1 reflects "No Impact at All" and a score of 10 reflects "Extensive Impact" to their organisation. For each of the 36 risk issues, we computed the average score reported by all respondents.

Commentary – Chief Audit Executives

CAEs see a riskier near- and long-term environment than do most of their colleagues in the executive suite. Of all C-level respondents to our latest Top Risks Survey, internal audit leaders ascribe the highest-magnitude ratings to risks they expect to challenge their organisation's ability to achieve its performance objectives during the next 12 months. CAEs also give the highest risk ratings among all C-suite leaders to issues they expect to challenge their organisations a decade out, in 2034.

The concerns that CAEs rate highest for these two time periods are nearly identical. They view cyber threats to be their top risk issue – and by a significant margin. Third-party risks are also a significant concern, especially considering they represent a rapidly expanding aspect of cybersecurity risk as organisations become increasingly data-driven and reliant on technology vendors. People- and technology-related issues round out the list of top CAE risk concerns at a time when talent management and technology enablement function as pivotal enablers of internal audit transformation and relevance.

Overview of top risks for 2024

Cyber threats stand out as the topmost risk concern for CAEs this year (versus ranking third in the overall global response), and internal audit leaders scored this risk issue much higher than their C-suite counterparts did on our 10-point scale, similar to what we have seen in prior years. In related research conducted by Protiviti and The Institute of Internal Auditors, more than 75% of CAEs and technology audit leaders reported that they consider cybersecurity to be a high-risk area.[2] These findings are understandable given the CAE's risk mindset along with the fluid nature of cyber risks and their repercussions. Without question, the cyber landscape has become more complex. The growth of malicious actors, including nation state and sophisticated collectives, utilising advanced techniques, from ransomware and phishing to SIM swapping, continues to raise the risks and stakes for organisations on multiple fronts, including regulatory ramifications and reputation management. The loss of customer and client data brings forth significant consequences, especially with the U.S. Securities and Exchange Commission's (SEC's) recently finalised disclosure requirements for public companies that have experienced a material cyber incident.

In July 2023, the SEC adopted amendments to its rules on cybersecurity risk management, strategy, governance and incident reporting by public companies.[3] With few exceptions, failure to report a breach within four business days could result in regulatory fines and scrutiny, elevating the organisation's exposure.[4] The SEC's cyber disclosure rule has significant effects on the internal audit function and annual audit plan, demanding a comprehensive cybersecurity risk assessment and plans to identify and communicate threats and breaches in a timely manner. It also is clear that security and privacy have become inextricably linked as organisations expand their use of cloud-based systems and other internet-connected devices, as well as increase their collection of data to support various business operations and priorities.

[2] *Navigating a Technology Risk-Filled Horizon: Assessing the Results of the Global Technology Audit Risks Survey*, Protiviti and The Institute of Internal Auditors, October 2023: www.protiviti.com/gl-en/survey/it-audit-survey.

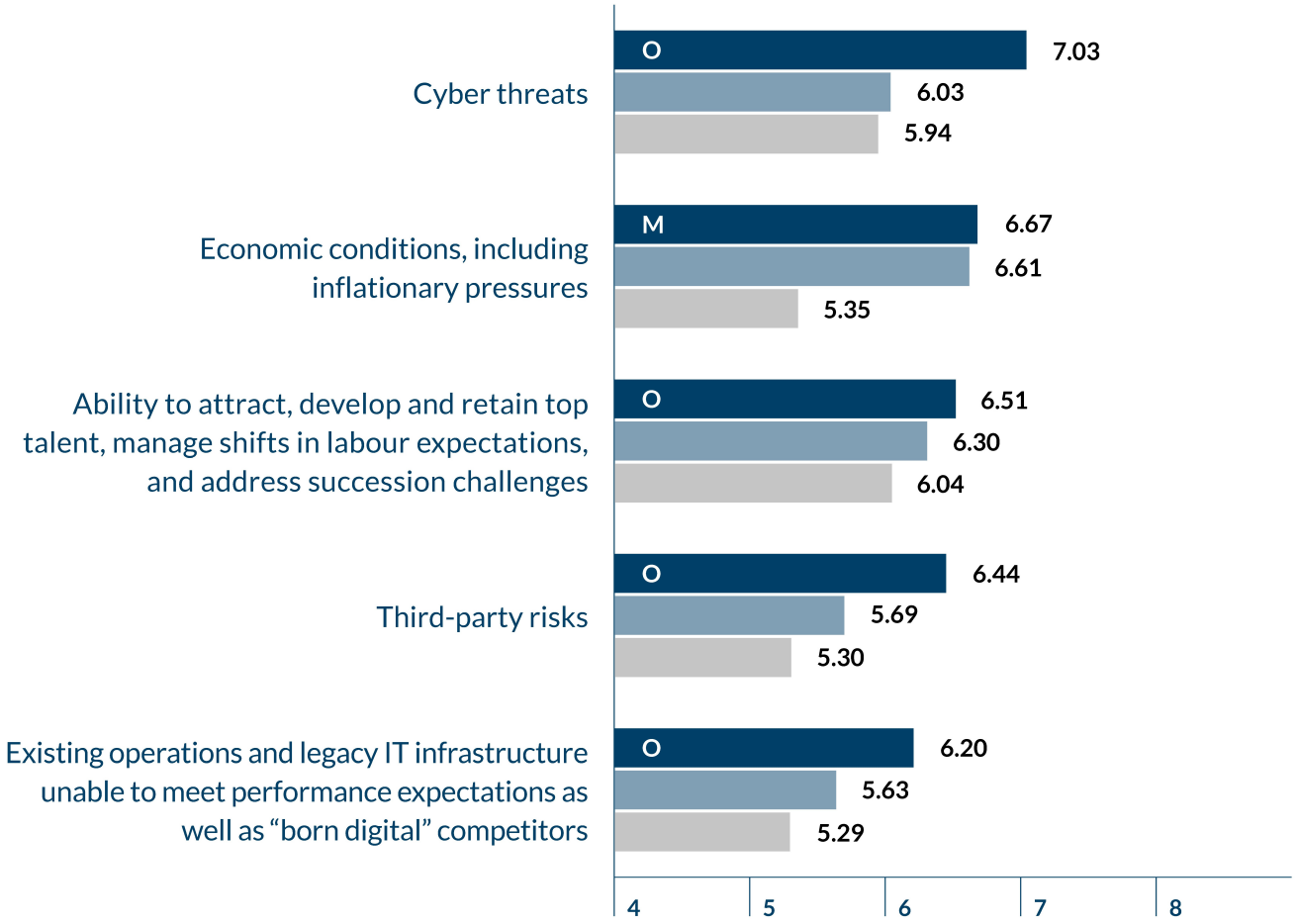
[3] "SEC Cybersecurity Disclosure Enhancements: Efforts to Boost Investor Confidence," Protiviti Flash Report, 2 August 2023: www.protiviti.com/us-en/flash-report/sec-cybersecurity-disclosure-enhancements-efforts-boost-investor-confidence.

[4] Specifically, an organisation must report a breach within four business days of when the breach is determined to have been material, the assessment of which should be reached without undue delay.

Thinking of these areas together is essential for CAEs and internal audit functions to work with management to address and mitigate potential cyber risks. In particular, as part of their mission to provide independent assurance that the organisation's risk management, governance and internal control processes are operating effectively, internal audit leaders should ensure that their leadership colleagues understand their cybersecurity-related responsibilities in the overall public and financial reporting process.

Other highly rated 2024 risk concerns for CAEs include economic conditions (including inflationary pressures), talent management and succession challenges, third-party risks, and risks related to aging or otherwise insufficient technology infrastructure.

CAEs — 2024



The magnitude and severity that CAEs ascribe to third-party risks in 2024 is substantially higher compared to their views of these areas in last year's survey. This growing importance reflects, at least in part, an understanding that third- and fourth-party risk management is an increasingly pivotal component of overall cybersecurity. Organisations continue to share more data with third parties as well as others in their ecosystem of vendors and other business partners. The importance of this shared data is rising as companies generate more business value

from this information, and this is compounded by heightening global regulatory scrutiny and stakeholder expectations related to trust and transparency. All of these factors make it imperative for stringent risk assessments of third-party providers. Fortunately, CAEs and their internal audit groups, given their enterprisewide responsibilities, maintain a clear picture of vendors the organisation relies on to support technology and data-related activities as well as a broader range of needs.

In regard to economic conditions, CAE views are not a surprise given the volatility in the global economy over the past 24 months. Even with some positive economic indicators emerging in early 2024, with inflationary trends easing, CAEs remain wary. A volatile geopolitical climate, unforeseen economic events and even the ongoing threat of natural disasters are among triggers that can pivot the economy downward. While there is more positive economic news (and we must try to avoid the trap of "talking ourselves" into a recession), CAEs and other business leaders understand that things can change fast. When considering, in particular, increasing geopolitical tensions and supply chain strains, along with many high-stakes national elections taking place across the globe this year, uncertainty about the economic outlook will likely continue throughout 2024.

The ability to attract, develop and retain top talent, manage shifts in labour expectations, and address succession planning remains a significant concern for CAEs. Their talent- and skills-related risk view pertains to the overall enterprise as well as their own internal audit function. Organisationwide, recruiting and retaining talent has become a greater challenge than ever. Competition is fierce, with fewer skilled professionals in the market. In the coming years, the challenges will become even greater as a baby-boomer generation of employees moves into retirement without a commensurate volume of talent entering the workforce to close the gap.

The ability to attract, develop and retain top talent, manage shifts in labour expectations, and address succession planning remains a significant concern for CAEs.

For CAEs, these talent and skills concerns extend to the internal audit function. A majority of CAEs experience difficulties accessing the talent they need to equip them to address the broad range of risk areas that often make their way onto internal audit plans, let alone allowing for sufficient focus on innovation and transformation activities. Internal audit leaders point to the ability to recruit qualified candidates and retain and upskill people as formidable performance inhibitors.[5]

Internal audit leaders identify two other technology-related issues as top risk concerns for 2024: existing operations and legacy IT infrastructure impeding the organisation's ability to meet performance expectations, and competition from "born-digital" organisations. Many CAEs are well aware that their "legacy" organisations continue to play catch-up while squaring off against more agile competitors in the market that have advanced, cloud-based technologies and other digital processes and capabilities baked into their enterprises. As organisations move through their technology modernisation initiatives, there are numerous opportunities for internal audit functions to engage with their business counterparts to help evaluate risk, provide assurance and deliver advisory services in these areas, as well as to become more involved in the organisation's broader transformation efforts.

Internal audit leaders also recognise that this risk extends to their domain and are increasingly looking within their own functions to determine what transformation and modernisation opportunities are possible, especially with the technology advancements we are experiencing. Investments in artificial intelligence and machine learning, advanced analytics, process mining, and cutting-edge automation are foundational drivers of internal audit transformation. These advanced tools also strengthen recruiting and retention activities, given that top internal audit professionals want to expand their skill sets, especially regarding their proficiency with advanced

[5] *Achieving Audit Relevance*, Protiviti, March 2023: www.protiviti.com/gl-en/survey/next-gen-ia-2023.

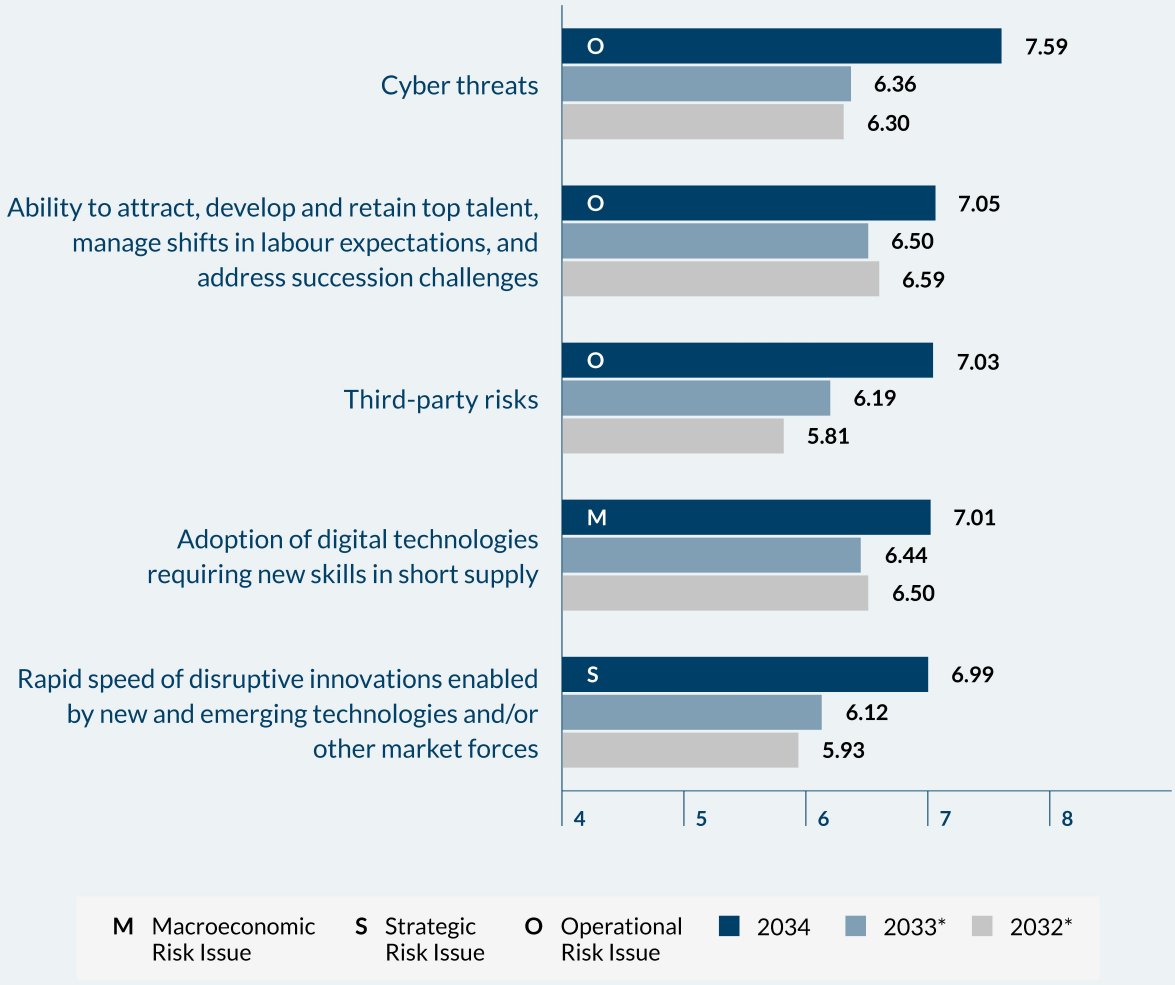
technologies. Legacy technology infrastructure and the resulting technical debt that must be managed can slow the adoption of these next-generation internal auditing tools, putting those internal audit functions at a disadvantage to born-digital competitors.

Overview of top risk issues for 2034

As the technical sophistication of cyber threats continues to advance and evolve, savvy CAEs know that, in all likelihood, their – and their third parties' – cyber defences will be breached at some point over the next decade. CAEs' 2034 risk concerns reflect this sobering realisation as cyber threats again occupy the top position by an even more significant margin compared to the 2024 risk ratings, and they are scored at a level much higher than that of global respondents. Third-party risks, including the cybersecurity threats they pose, also rank as a top CAE concern for 2034.

Compared to their 2024 assessments, CAEs give notably higher risk ratings to all of their top 2034 concerns, which, in addition to cyber threats and third-party risks, include talent management and succession planning, skills availability, and the rapid speed of disruptive innovation driven by emerging technologies.

CAEs — 2034



* This data was reported as 2032 and 2031 results, respectively, in our prior year reports. We have shifted our terminology to reflect a decade out, thus have revised these year references in the interests of clarity.

In addition to overall talent recruiting and retention concerns, internal audit leaders single out access to skills related to the adoption of digital technologies as a critical risk issue. This challenge affects the entire organisation, including the internal audit group, where ongoing transformation and the function's core value rely heavily on its ability to implement advanced auditing technologies. Doing so requires CAEs and other internal audit leaders to access the talent and skills needed to use and optimise those tools. This need will only intensify over the next 10 years as new technological breakthroughs produce more disruptive innovations at an even faster pace than they are currently materialising.

Internal audit leaders single out access to skills related to the adoption of digital technologies as a critical risk issue.

Time will tell if the 2034 outlook holds, although several of the 2024 top risks will undoubtedly remain present 10 years from now. Considering the 10-year time horizon can be helpful to challenge the near-term thinking that often dominates risk discussions and drive more of a horizon-scanning and out-of-the-box approach to the risks that will be critical in 2034 and beyond.

Call to action for CAEs and internal audit leaders

As CAEs address their risk concerns while advancing internal audit transformation and their pursuit to optimise their value and relevance, they should update their talent management mindsets and activities to reflect the new labour market realities. They also should ensure the internal audit function and enterprise have the right level of focus and attention on cybersecurity, third-party risk and overall economic conditions. Here are a number of calls to action for CAEs and internal audit leaders to address these areas.

Cyber threats – Organisations should focus on implementing multi-layered security control measures, including employee training on recognising phishing attempts, deploying advanced malware detection and security monitoring systems, and establishing robust incident response plans. Regular security audits and compliance checks should be conducted to align with the latest SEC guidelines, as well as to focus on testing the effectiveness of incident response and recovery capabilities.

Third-party risk – CAEs should advocate for the implementation of comprehensive third-party risk management programs that include due diligence processes, ongoing monitoring of third-party security practices, and the integration of third-party risk into the organisation's overall risk management framework. Organisations should establish clear contracts that outline the cybersecurity expectations and requirements for third parties.

Talent – In addition to offering competitive compensation packages, organisations should develop a strategic talent management plan that emphasises career development opportunities, the employee experience, upskilling/reskilling programs, and a strong organisation culture that values diversity, inclusion, and professional and personal development.

Economic conditions – To navigate continued uncertainty in the global markets, CAEs should work with executive management to develop flexible financial and operational strategies that can adapt quickly to changing economic conditions. CAEs can ensure that their audit plans (as well as individual audits or advisory projects) have an appropriate focus on driving operational efficiency as well as a focus on opportunities for, as well as potential impacts of, cost containment and related measures.

About the Executive Perspectives on Top Risks Survey

We surveyed 1,143 board members and executives across a number of industries and from around the globe, asking them to assess the impact of 36 unique risks on their organisation over the next 12 months and over the next decade. Our survey was conducted in September and October 2023. Respondents rated the impact of each risk on their organisation using a 10-point scale, where 1 reflects “No Impact at All” and 10 reflects “Extensive Impact.” For each of the 36 risks, we computed the average score reported by all respondents and rank-ordered the risks from highest to lowest impact.

Read our Executive Perspectives on Top Risks Survey executive summary and full report on the Protiviti or NC State University ERM Initiative websites.

Contact

Andrew Struthers-Kennedy
Managing Director
Global Leader, Internal Audit and Financial Advisory
andrew.struthers-kennedy@protiviti.com