2026 EDITION

EXECUTIVE PERSPECTIVES ON TOP RISKS AND OPPORTUNITIES

protiviti®
Global Business Consulting

Growth, talent, resilience and AI are top-of-mind for CAEs

By Andrew Struthers-Kennedy and Angelo Poulikakos

CAEs continue to face challenges in balancing competing priorities: enterprise growth versus control, speed versus assurance, AI excitement and enablement versus AI governance, to list just a few.

Over the last 13 years, we have issued annual research reports on the top risks faced by leaders all over the world. This year, we have added an emphasis on opportunities to set the tone for identifying and responding proactively to emerging trends, market shifts and evolving customer expectations. Organizations that balance risk management with a focus on growth are better equipped to innovate products and services, enhance their resilience, adapt to change, and achieve top-line growth and strategic differentiation. It is all about unlocking opportunity; managing the downside while capturing the upside.

Our 14th annual **Executive Perspectives on Top Risks and Opportunities Survey** contains insights from 1,540 board members and C-suite executives around the world regarding their views on:

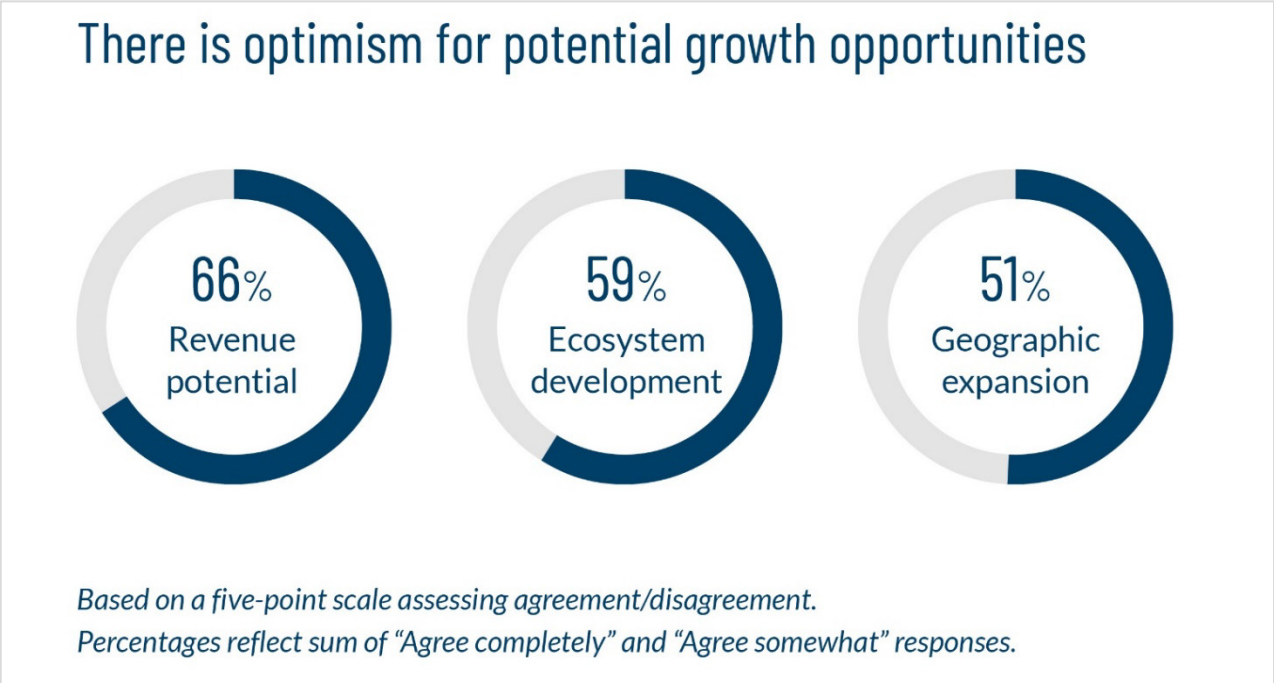
- Three specific areas for growth considering the current environment;
- Opportunities and challenges associated with the transformative impact of artificial intelligence (AI) on their organizations;
- The top risks on the horizon for the near-term (two to three years ahead) related to 28 specific risks across three dimensions (macroeconomic, strategic and operational) and for the long-term (a decade from now) related to 12 risk themes that consider the strategic and operational near-term risks; and
- A discussion of their organizations' near-term strategic investment priorities, given the opportunities and the risks they face.

Our survey participants shared their views through an online survey conducted from early September through mid-October 2025. This paper offers specific insights into these issues from the perspective of the chief audit executive (CAE).

Where do CAEs see the greatest opportunities for their organization over the next two to three years?

Like most executives, CAEs are optimistic about the **transformative impact of technology** – particularly AI, which is lowering barriers to entry across industries and geographies and creating immense revenue potential. However, they also see AI and other emerging technologies introducing new – and exacerbating existing – risks that organizations must manage effectively.

From an audit and risk perspective, these developments underscore the need for CAEs to recalibrate their risk lens and align audit activities tightly with strategic priorities. Growth initiatives often hinge on areas that, historically, may not have been part of the audit plan – such as experimentation with and implementation of emerging technologies, expansion of ecosystem partnerships, and introduction of data-driven products and services. For CAEs, leaning into these strategic areas – providing both assurance and advisory support – is critical, even if they fall outside traditional "auditable" areas within internal auditors' comfort zones.



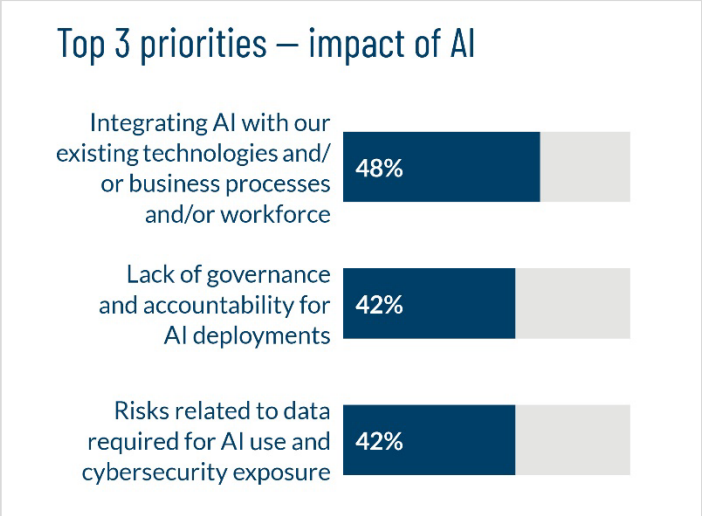
Data, in particular, is a foundational component of growth. As organizations increasingly view data as a form of currency, new products and services will depend heavily on the quality of that data. Poor data quality can be linked directly to failed AI initiatives, and more broadly to both risk management challenges and the inability to capitalize on market opportunities. This makes it essential for internal audit teams to **strengthen their capabilities in auditing data governance and integrity**, such that they are able to communicate clearly – and with credibility – the challenges the organization needs to overcome. Investing in data-related skills, including those focused on governance considerations and leading practices, remains a priority area for CAEs and their internal audit functions to address.

Ecosystem partnerships also introduce third-party risk – a top near-term risk concern for CAEs. (See below.) As organizations make big bets on partnerships to accelerate growth, CAEs must ensure **robust oversight of third-party relationships** as well as fourth- and *n*th-party relationships, mitigating risks that could undermine strategic objectives.

One final point: Internal audit must align its audit plan and activities to the organization's strategic priorities – such as data governance, technology modernization, AI implementation and talent. This alignment must be a top priority for the CAE, as it's a critical expectation of executive stakeholders.

What will be the organization's most significant challenges regarding the impact of AI over the next two to three years?

For CAEs, the most significant AI-related challenge is **integration** – specifically, plugging AI into existing technologies, business processes and the workforce. These concerns underscore the challenges of fitting AI into architectures and operating models that were not designed for it. Many organizations, in effect, are "jamming" AI into legacy systems and data lakes, amplifying risk rather than unlocking value, while AI-native competitors move faster and more coherently as they establish cultures that foster innovation and agility. In short: The greatest AI risk is not necessarily misuse but poor integration in environments that were never designed, nor are ready, for AI.



CAEs need to support enterprise initiatives that drive innovation and speed while balancing them through controls – enabling safe growth and acceleration rather than inhibiting progress. The reality is that **AI is moving faster than governance, standards and regulations**. Governance audits continue to reveal gaps and immaturity, even as AI influences key decisions affecting customers and employees. This calls for CAEs to emphasize flexible, value-oriented audit approaches (versus reactive compliance measures).

Data quality and governance are foundational fault lines. A significant source of AI risk stems from poor data and operating environments that were never prepared for AI. As new AI-enabled products and services depend on trustworthy data, CAEs must elevate assurance around data lineage, integrity, stewardship and access – capabilities that are currently scarce – as well as around critical cybersecurity protections.

Internal audit also will face headwinds in moving beyond high-level AI governance reviews into **deployment-level assurance**, which demands developing a clear audit roadmap. Among the key components of this roadmap are risk-ranking AI use cases, understanding how models were developed, evaluating training data and treating AI like an application control – testing inputs, outputs and automated

decisions, and verifying management oversight. Today, that depth is largely absent, even in SOX work, where AI's role in controls is seldom questioned.

Finally, with expanding risk surfaces resulting from AI deployments, resource capacity and cost pressures collide. Internal audit should **accelerate routine work with AI** to free capacity to address emerging AI risks. CAEs must lean in – recalibrate the risk lens, align audit to strategic priorities and ensure the organization can adopt AI swiftly and safely.

What are the most significant short-term (two to three years) concerns and risks on the minds of CAEs?

CAEs see their organizations being tested on two fronts: **managing the governance gap as AI adoption accelerates** and **addressing the talent transformation** required to thrive in this new environment. Both risks are intertwined and demand proactive, strategic engagement from internal audit leaders. At the same time, cyber threats and heightened regulatory scrutiny are perennial risk concerns that CAEs understandably rank as significant.

Top global near-term risks – CAEs

2026 rank	Risk issue	Average*	2025 rank
1	Cyber threats	3.73	1
2	Heightened regulatory change, uncertainty and fragmentation	3.49	6
3	Third-party risks	3.47	3
4	Emergence of new risks from implementing AI	3.39	8
5	Skills and talent acquisition and retention, leadership development and succession challenges	3.37	2

* Average based on a five-point scale where 1 reflects "No impact at all" and 5 reflects "Extensive impact."

Concerns over cyber threats reflect the growing number of attacks coupled with the rapid rise of AI adoption and, as a result, even greater exposure to these threats. For CAEs and internal audit functions, assuring that management is focused on fortifying the enterprise's cybersecurity posture remains a top priority.

The global **regulatory landscape continues to see dramatic shifts**, including but not limited to U.S.-driven deregulation. At the same time, the international regulators continue to introduce new guidelines and are monitoring organizations closely. Bottom line, business leaders are relying on CAEs and internal audit teams to assist in interpreting risks around regulatory compliance requirements and to provide independent assurance as to compliance posture and readiness.

While the sharp rise in AI implementation concerns is unsurprising, it represents an inflection point for CAEs: **providing governance and assurance over AI and supporting safe enterprise adoption, while simultaneously leveraging AI within their own functions**. This requires a fundamental rethink of audit

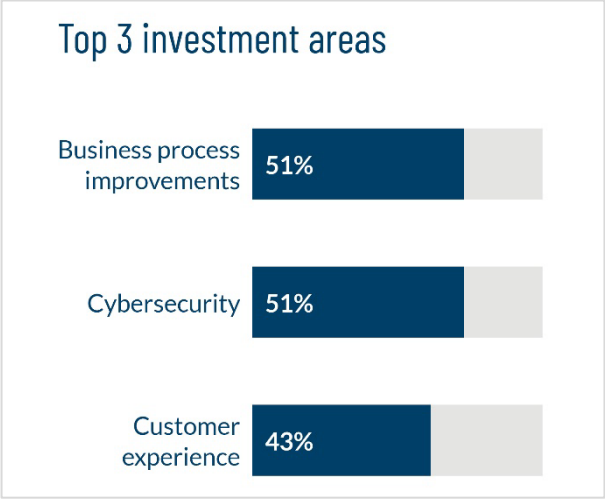
methodologies, risk frameworks and even cultural norms. AI is moving faster than governance structures can adapt, creating pressure to balance speed and control. Organizations that fail to deploy AI at a competitive pace risk falling behind, yet rushing AI integration into legacy systems and processes amplifies operational and data risks. For CAEs, this means leaning into areas that were once outside traditional audit plans, such as AI governance, data integrity and deployment-level assurance.

Equally concerning – though less visible among the top risks – is talent. The decline in talent-related risk perceptions may reflect short-term improvements in the labor market. However, this masks a deeper issue: readiness for the AI era. **Workforce strategy, upskilling and reskilling are existential challenges for internal audit teams** and the broader enterprise. While availability of resources may no longer dominate today's conversations, the real question for CAEs is whether the organization, and especially the internal audit function, have the right skills for the future.

For these and other near-term risk concerns, it's critical for the CAE to optimize both coverage (the breadth of risks, business areas and initiatives addressed) and assurance as to the depth of those activities, while providing the audit committee with clear visibility into what internal audit and other assurance functions are covering. This ensures strong alignment, communication and coordination across the risk landscape.

Based on these near-term risk issues, in what areas is the organization likely to invest the most over the next two to three years, and why?

CAEs see their organizations concentrating investments in three primary areas over the next two to three years: **business process improvements**, **cybersecurity** and **customer experience**, with human capital and infrastructure modernization closely linked to these priorities.



Business process improvements are often tied to large-scale transformation initiatives and reflect a broader focus over the past year on achieving greater efficiencies. These efforts frequently intersect with technology modernization – addressing technical debt, upgrading core infrastructure and embedding automation. For internal audit, these areas are an opportunity to **expand advisory engagements beyond traditional assurance**.

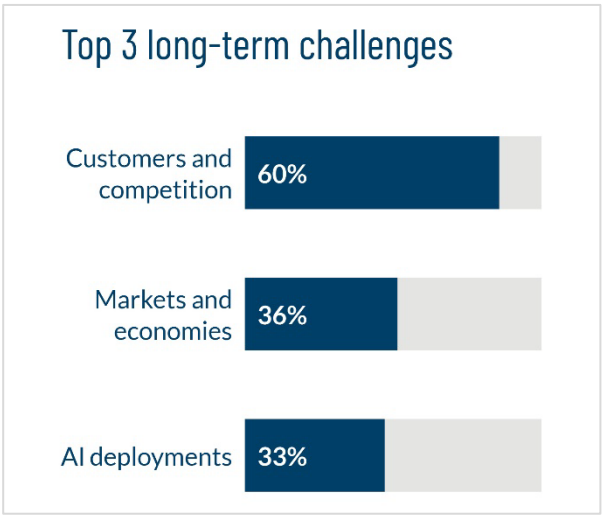
Cybersecurity remains a consistent focus, though the nature of investment is shifting. After years of heavy spending on protection capabilities, **organizations are now emphasizing detection and response**. This pivot reflects fatigue around "unlimited budgets" for cyber, but it's a mistake to assume the risk has diminished. On the contrary, AI is fundamentally altering the cyber threat landscape – creating new attack vectors and amplifying vulnerabilities at unprecedented speed. Quantum computing is another emerging cyber threat. (More on this below.) These challenges underscore the importance of evolving cybersecurity strategies alongside AI adoption.

Human capital, while less visible among the priority investment areas, is equally critical. **Workforce upskilling and reskilling**, as part of a broader workforce strategy rethink and organization chart redesign – both within internal audit and across the enterprise – are essential to enable success in an AI-driven environment and assure future-readiness. The decline in talent-related near-term risk perceptions (as noted earlier) may mask the urgency of this challenge. Organizations that fail to invest in learning and development will struggle to adapt.

How do CAEs view the 10-year risk outlook for their organization?

Long-term, CAEs see a mix of macroeconomic uncertainty and more controllable strategic and operational challenges. At the top of their minds are **customers and competition** – areas that demand organizations not only set strategies focused on resilience but also execute consistently to maintain relevance. While competitive dynamics cannot be controlled, positioning and differentiation can.

Markets and economies represent the most uncontrollable element of the long-term outlook. Global volatility, economic cycles and geopolitical shifts will continue to shape the environment, but **organizations can mitigate exposure through agility and resilience** – areas for which internal audit can assess and advise. This raises another critical theme: organizational culture and resilience. The ability to absorb shocks, pivot quickly and sustain performance is a defining long-term risk factor.



Talent and technology also permeate the long-term conversation. The pace of technological change, particularly AI, will reshape roles and processes within a decade, but its implications for governance and ethics will persist well into the future.

Quantum computing, while only garnering a small response, also deserves attention. Its low ranking likely reflects limited understanding rather than low risk. Over the long-term, **quantum computing represents a potential game changer** – one that could upend cybersecurity, encryption and competitive advantage. While it is not an immediate threat, its eventual impact could be profound. CAEs must ensure their organizations monitor developments and prepare for the disruption it will bring.

Guidance/call to action for next two to three years

Following are calls to action for CAEs as they help their organizations and internal audit functions navigate the changing landscape.

- **Recalibrate the risk lens around AI and emerging technologies.** Align audit plans with strategic priorities by incorporating into the audit scope AI governance, deployment-level assurance and data integrity. Move beyond high-level reviews to evaluate AI models, training data and automated decision-making processes. Provide a view independent from management's perspective on the holistic regulatory environment and how it may change in the future.
- **Strengthen data governance and cybersecurity assurance.** Treat data as a strategic asset. Elevate assurance around data lineage, integrity and stewardship while reinforcing cybersecurity controls to address new AI-driven attack vectors. At the same time, think more long-term and prepare for emerging threats like quantum computing.
- **Embed internal audit in growth initiatives.** Expand audit coverage to areas historically outside the audit plan – such as ecosystem partnerships, digital transformation and customer experience initiatives. Deliver proactive risk insights and governance support to enable innovation while mitigating third-party risks.
- **Accelerate internal audit's own AI adoption.** Leverage AI to automate routine audit tasks and free capacity for emerging risk areas. Position internal audit as a leader in responsible AI use by demonstrating how technology can enhance efficiency and insight without compromising control.
- **Champion workforce upskilling and talent strategy.** Advocate for and support enterprisewide reskilling initiatives to prepare for an AI-driven future. Ensure internal audit teams acquire capabilities in AI risk assessment, data analytics and technology governance to remain relevant and add strategic value. At the same time, the team must focus on the continued, or even accelerated, development of uniquely humanistic qualities – such as ethical judgment, empathy, critical thinking, relationship building and more – that will not be easily (if at all) replaced or replicated by AI and therefore will become ever more important in the AI-era.
- **Advise on infrastructure modernization and process improvements.** Partner with management on modernization initiatives tied to technical debt reduction, automation and process optimization. Provide both assurance and proactive advisory that these transformations strengthen resilience and align with long-term strategic objectives.
- **Monitor long-term disruptors and build organizational resilience.** Incorporate forward-looking risk assessments into audit planning, including in high-impact areas such as quantum computing and global volatility. Advise on cultural and structural resilience to help the organization pivot quickly and sustain performance amid uncertainty.

About the authors

Andrew Struthers-Kennedy is Protiviti's Global CAE Solutions leader. In this role, Andrew's focus is on understanding and advancing the strategic priorities and transformation agendas of CAEs and their leadership teams, as well as those of their executive and board stakeholders. Andrew is inspired by and committed to helping to advance the profession, raising the global brand and profile of internal audit and helping ensure the profession, its leaders and practitioners get and remain future ready.

Angelo Poulikakos is Protiviti's Global Internal Audit and Financial Advisory capability leader. Angelo's focus is on driving the modernization of assurance, risk and controls with AI, automation, analytics and intelligent tooling while supporting the shift of audit and risk from retrospective reviews to forward-looking insight. He works with clients to build programs that are faster, more reliable and board-ready, retaining a strong focus on governance and quality.