The capability questions every CAE should ask

Chief audit executives (CAEs) broadly share the priorities of other board members and C-suite leaders, but their results reveal a distinct perspective on where organisational capability is most likely to be tested.

Like the broader respondent population in the survey, CAEs identify cyber threats and risks arising from AI implementations as their leading near-term concerns, place workforce enablement at the centre of AI value realisation, and express less confidence in their organisations' ability to respond than in their ability to transform or protect. The differences are equally instructive. CAEs place greater emphasis on third-party risk, AI governance and accountability, and investments in cybersecurity and business process improvement.

Taken together, the results suggest CAEs see the future through a capability and dependency lens; specifically, whether the organisation has the governance, talent, data, relationships and decision-making structures required to capture opportunities and respond as conditions change.

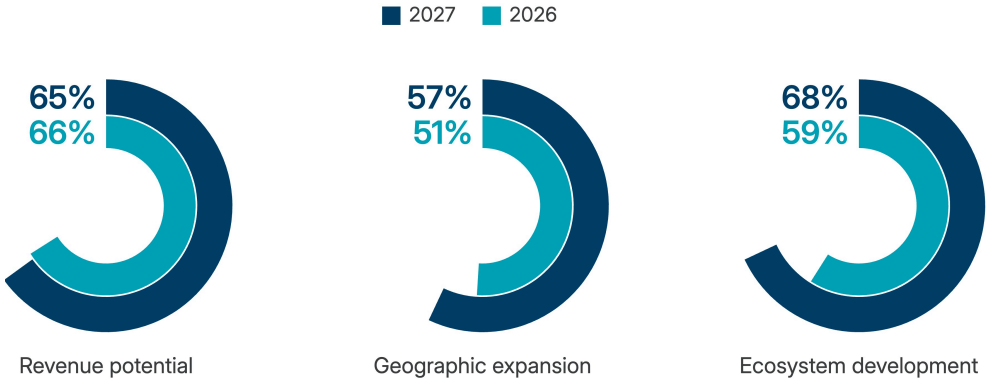
The research also reveals broader capability challenges. AI demands governance and workforce readiness. Third-party relationships add dependencies. Talent and capability gaps weaken execution, oversight, decision-making and adaptability. Data, analytics and technology can accelerate the response, but only when leadership, culture and operating models are aligned and flexible enough to support change. These issues are not isolated; they compound one another.

For CAEs, the takeaway is clear: Internal audit must look beyond individual risks and assess whether the organisation can sense change, make timely decisions, and mobilise the capabilities required to capture opportunities, protect value and remain resilient. This reinforces internal audit's broader evolution from retrospective assurance toward risk and decision intelligence: providing timely, decision-useful risk context, grounded in independent judgment, while outcomes can still be influenced.

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

Ecosystem development is viewed as the leading growth opportunity, suggesting CAEs see increasing value in collaboration, technology ecosystems and external capabilities. Geographic expansion also moved higher despite continued geopolitical uncertainty and economic volatility, while the percentage identifying significant revenue growth opportunities remained essentially unchanged.

Views about opportunities for growth – CAEs



68%

view ecosystem development as an organisational growth opportunity in the near-term.

CAEs are somewhat more optimistic about growth opportunities than the broader respondent population: 68% identify ecosystem development as a significant opportunity, compared with 65% overall, while 57% see opportunities for geographic expansion, compared with 52% overall. Views on revenue potential are nearly identical at 65% for CAEs and 64% overall.

More significantly, CAEs rank third-party risk as their third-highest near-term concern, compared with eighth overall (see near-term risk concerns section below). Their results highlight both sides of ecosystem growth: the opportunity to access new capabilities and markets, and the need to govern

the resulting dependencies across partners, platforms, technology providers and data flows.

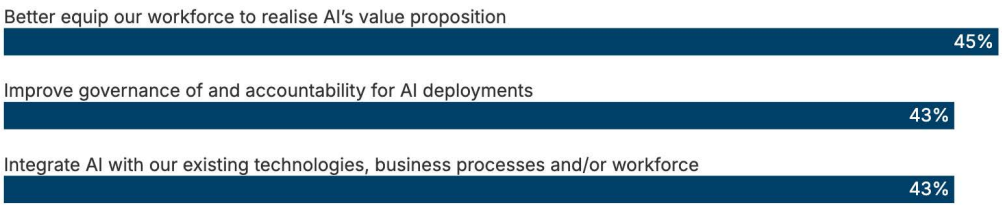
A question for CAEs: Are we governing ecosystem dependencies with the same discipline applied to capabilities we own and operate directly?

What priorities do CAEs see as most important to maximising the value of AI deployments?

For CAEs, the challenge has shifted from whether or how organisations will adopt and deploy AI to whether they also can govern it, integrate it and equip people to convert its capabilities into measurable results.

CAEs and other executives are closely aligned on the capabilities required to maximise AI's value. Workforce enablement ranks first for both groups, followed by integration with existing technologies, processes and the workforce, and stronger governance and accountability. CAEs place greater emphasis on governance: 43% select it as a leading priority, compared with 38% overall. Among CAEs, governance is tied with integration, reinforcing the importance audit leaders place on clear accountability and disciplined execution.

Top AI opportunities – CAEs



These findings signal a shift beyond experimentation. Access to AI tools is not enough. Organisations need employees who can apply them effectively, operating models that embed them into established workflows and governance structures that direct resources toward the most valuable use cases.

Enabling teams remains central to maximising AI value, both within internal audit and across the enterprise. The challenge is now about more than adoption; it's about redesigning workflows, equipping people to use AI effectively, and determining where to build, buy or source capabilities. The opportunity for internal audit functions is to move beyond using AI to

accelerate existing tasks and rethink how work is structured, performed and reviewed.

That distinction matters because the greater risk is not slow adoption, but rather shallow adoption that adds tools without materially changing workflows, capabilities or outcomes. As technology assumes more routine execution, the differentiating internal audit capabilities shift toward human judgment, critical thinking, professional scepticism, communication, and the ability to interpret and challenge technology-generated outputs. These capabilities will not develop automatically. CAEs need to build them deliberately through continued learning, varied experiences, coaching and new development pathways.

Governance plays a direct role in generating returns, not simply ensuring appropriate oversight and control. In many organisations, governance is still developing alongside rapidly expanding AI adoption, but the two should not be viewed as competing priorities. Governance should help the organisation prioritise AI use cases, establish ownership, align investment with strategic value and define how results will be measured. Protiviti's AI Pulse Survey reinforces the connection between governance and value: Organisations confident in their data are three times more likely to exceed AI ROI expectations, with governance, training and transparency identified as the foundations of that confidence.

In this light, the key question is no longer whether governance is keeping pace with deployment. It is whether governance is helping management concentrate resources on the deployments most likely to improve performance and create sustainable value. Evidence may include improvements in cycle time, coverage, quality, capacity or decision effectiveness, as well as clear distinctions between scaled use cases, pilots and low-adoption deployments.

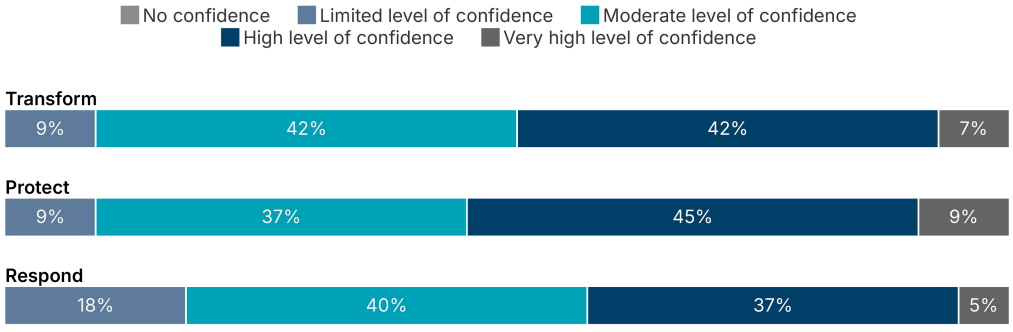
A question for CAEs: Can management demonstrate where AI is creating measurable value, not merely where it has been deployed?

Governance should help the organisation prioritise AI use cases, establish ownership, align investment with strategic value and define how results will be measured.

We asked CAEs three specific questions about their views on the organisation's ability to (1) transform the enterprise, (2) protect enterprise value, and (3) respond with agility to market opportunities and risks. What did they tell us?

An organisation's ability to respond may be the clearest test of its resilience. CAEs and the broader respondent population share the same confidence pattern: Leaders are more confident in their ability to protect and transform than in their ability to respond with agility. CAEs are somewhat more confident across all three dimensions, with 54% reporting high or very high confidence in protection, 49% in transformation and 42% in response, compared with 48%, 45% and 38%, respectively, for the overall population.

Views about the ability to transform, protect and respond – CAEs



54%

have a high level of confidence in the organisation's ability to protect enterprise value.

The response gap is also evident at the lower end of the scale: 18% of CAEs report limited confidence in the organisation's ability to respond to market opportunities and risks, twice the percentage reporting limited confidence in either transformation or protection. Transformation and protection often benefit from structured programs, established governance and deliberate investment. Response capability is tested under different conditions and requires the organisation to recognise change, interpret its implications, make a timely decision and mobilise before options narrow.

These gaps have broad implications for organisational resilience. Effective response depends on more than crisis plans and established controls. It requires experienced leadership, the right people in the right roles, timely access to reliable information and the ability to prepare for multiple scenarios. Concerns expressed in the survey around talent, AI, third parties

and data analytics reinforce the interdependence of these capabilities. No single investment or control can make an organisation resilient if its people, information and decision-making structures cannot work together, under pressure, to respond effectively when opportunities arise or risks emerge.

For CAEs, response readiness can be evaluated through three connected capabilities: Can the organisation **sense**, **decide** and **mobilise**?

- **Sense:** Detect material changes, emerging risk signals and decision triggers early.
- **Decide:** Interpret the information, understand the trade-offs and exercise clear decision rights.
- **Mobilise:** Coordinate people, resources and operations quickly enough to affect the outcome.

Assurance over individual controls and risks remains necessary, but it may not reveal whether these capabilities will work together under pressure.

A question for CAEs: Do leaders know the decision triggers, information and authorities required to act before options narrow?

What are the most significant near-term concerns and risks on the minds of CAEs?

CAEs see an overall riskier near-term environment than they did in the prior year's survey. They also are confronting risks that are more interconnected, more dependent on organisational capability and less susceptible to being managed individually. Weaknesses in one area can compound exposures in another.

Cyber threats remain the leading near-term concern for CAEs, continuing a pattern seen in prior years. Risks associated with implementing AI posted one of the largest increases in the survey and now rank second. Third-party risks, talent and succession challenges, and regulatory uncertainty round out the top five.



Top five near-term risks – CAEs

Risk description	2027	2026
Cyber threats	3.76	3.73
Emergence of new risks from implementing AI	3.67	3.39
Third-party risks	3.64	3.47
Skills and talent acquisition and retention, leadership development and succession challenges	3.41	3.37
Heightened regulatory change, uncertainty and fragmentation	3.41	3.49

CAEs align closely with the broader respondent population in ranking cyber threats and risks arising from AI implementation first and second. Beyond those two concerns, their priorities diverge. Third-party risk ranks third for CAEs but eighth in the overall results, while talent and succession challenges rank fourth for CAEs but sixth overall. The broader population places greater emphasis on economic conditions and disruptive innovation. This contrast suggests CAEs view the near-term environment through a more pronounced protection and dependency lens.

What makes these risks particularly challenging is their interconnected nature. AI introduces new governance and accountability requirements. Third-party providers are deploying AI-enabled tools and services that create additional dependencies. Cybersecurity exposures, from data to infrastructure access, extend across supplier and technology ecosystems. Talent and capability gaps affect an organisation's ability to govern, oversee and respond to these evolving risks. Regulatory requirements influence how all these activities are managed. Rather than representing isolated concerns, many of the top-ranked risks reinforce and amplify one another.

Several of the notable year-over-year changes reinforce this interconnectivity pattern. AI implementation risks, third-party risks, privacy concerns and data analytics capabilities all rose in significance, pointing to a broader capability-risk challenge.

For CAEs, the implications for internal audit extend beyond individual risk rankings. Traditional assurance remains essential, but organisations also need insight into how risks connect and compound across the enterprise. Traditional episodic coverage may be structurally mismatched to risks that move and compound faster than the audit cycle. Internal audit needs



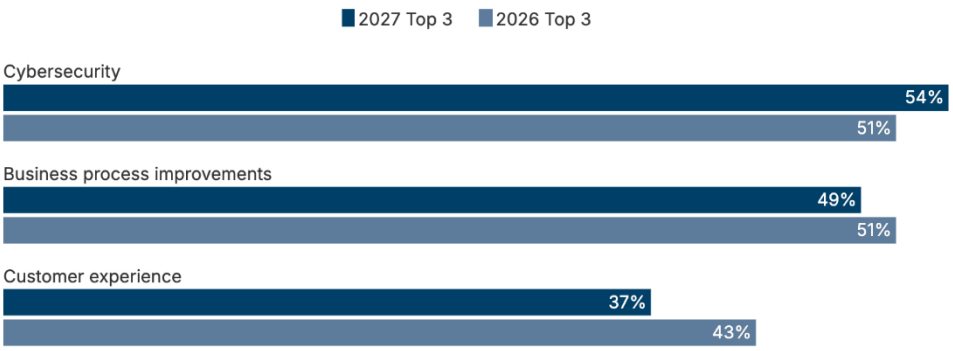
stronger risk sensing, more dynamic planning and explicit triggers for reconsidering coverage as conditions change.

A question for CAEs: Does our assurance model account for the speed at which interconnected risks can compound?

Given these near-term risk issues, where do organisations plan to invest most?

The investment results show greater emphasis on foundational capabilities that can address multiple risks, including cybersecurity, business process improvement, infrastructure modernisation and advanced analytics.

Top strategic investment priorities – CAEs



54%

rank cybersecurity as a top strategic investment priority.

While cyber threats, AI implementation concerns, third-party risks and talent challenges dominate the risk agenda, planned investments are concentrated in cybersecurity, business process improvement, customer experience, infrastructure modernisation and advanced data analytics. This suggests organisations are focusing less on solving individual problems and more on strengthening the capabilities required to navigate a more complex risk environment.

Cybersecurity remains the leading investment priority, mirroring its position as the top near-term risk. Beyond cyber, however, the investment pattern tells a broader story. Business process improvement ranks second, while infrastructure modernisation, data analytics and data privacy all gained ground year over year. These priorities indicate a focus on strengthening the systems, processes and information flows that support decision-making, resilience and performance across the enterprise.

The results raise questions about how closely investment aligns with stated risk and capability concerns. Third-party risk ranks third among CAEs' near-term concerns, yet third-party management ranks 10th out of 12 investment areas and declined year over year. Talent and succession rank fourth among near-term concerns, while investment in human capital management and workforce skilling also declined. Further, while response is the capability in which CAEs express the least confidence, crisis management ranks last among the listed investment areas.

Broader investments in technology, process improvement, infrastructure and analytics may address portions of these needs. The results do not establish, however, whether these investments are adequately strengthening third-party oversight, workforce capability or response readiness. That is precisely the question internal audit should help leadership examine. The prominence of business process improvement also suggests that CAEs see capability-building, rather than isolated remediation, as a central investment response.

The workforce results reveal another tension. CAEs identify workforce enablement as the leading priority for maximising AI's value, yet investment in workforce skilling declined year over year. Talent acquisition, retention, leadership development and succession remain among CAEs' five leading concerns and increased year over year, while concerns about general labour availability and access to emerging technology skills declined.

Technology may expand capacity, but sustainable value ultimately depends on people, reinforcing the need to look beyond staffing levels toward the leadership, judgment and adaptability required to govern, deploy, challenge and use technology effectively. Differences in perspective across leadership do not necessarily indicate that one group is wrong, but they reinforce the need for a shared view of the capabilities required and how investment decisions will build them.

A question for CAEs: Are resources aligned with the risks that matter most to leadership?

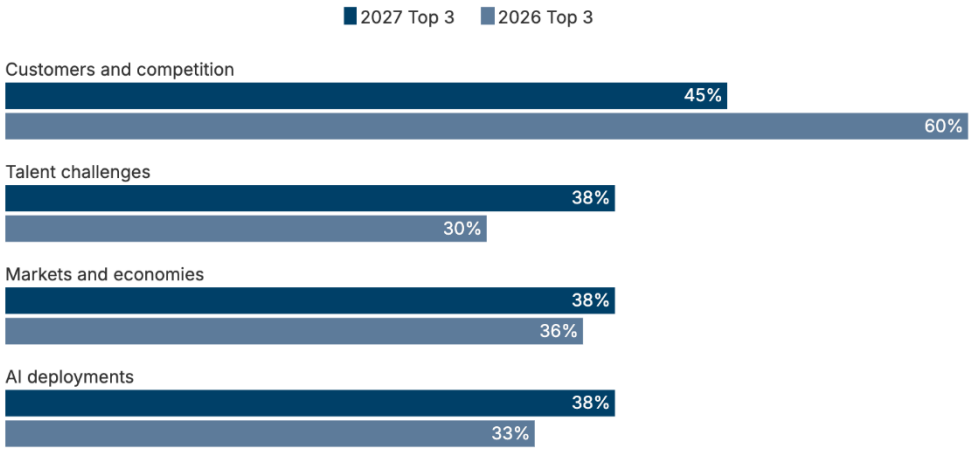


How do CAEs view the 10-year risk outlook for their organisation?

The most notable shifts in the 10-year outlook point to the capabilities organisations will need to remain resilient, relevant and effective in a more complex environment.

Customers and competition remain CAEs' leading long-term concern, but the 15-point decline from the prior year is notable. At the same time, talent challenges and AI deployments each rose to 38%, while organisational resilience and culture increased from 27% to 36%. The results point to a broadening of the long-term agenda: CAEs remain focused on strategic relevance and competition, but increasingly recognise that talent, technology, culture and resilience will determine whether the organisation can adapt over time.

Top long-term risks – CAEs



45%

view customers and competition as a top long-term risk theme.

CAEs and the broader respondent population share four leading long-term concerns: customers and competition, talent challenges, markets and economies, and AI deployments. The relative emphasis differs. Customers and competition rank first for CAEs at 45%, compared with 37% overall, while security and privacy lead the overall results at 41% but do not appear among the four highest CAE themes. This reveals an important contrast: CAEs' near-term priorities lean toward protection and organisational dependencies, while their 10-year outlook places greater emphasis on strategic relevance and competitiveness.

AI deployments and organisational resilience reinforce the same theme. AI represents a long-term capability challenge involving governance, workforce enablement, decision-making and organisational adaptability. CAEs recognise that resilience depends not only on systems and controls, but also on leadership, decision-making, culture and the ability to operate through continuous disruption.

For CAEs, the key long-term question is whether today's investments in talent, technology, governance and operating models are building the capabilities the organisation will need to remain competitive and relevant over time. Continued upskilling and reskilling may be the difference maker for internal audit. Technical and data fluency will matter, alongside adaptability, judgment, critical thinking, professional scepticism and the ability to translate complex signals into decision-useful insights. These capabilities will determine whether technology expands internal audit's intelligence and impact or simply accelerates existing work.

A question for CAEs: Are today's talent and technology investments building the capabilities the organisation will need in the future?



Calls to action for CAEs

- **Assess response readiness.** Determine whether the organisation can sense change, make timely decisions, and mobilise leadership, data, talent and operations when conditions shift.
- **Bring assurance and intelligence closer to decisions.** Use ongoing risk sensing, explicit audit-plan reconsideration triggers and earlier internal audit involvement to provide timely, decision-useful risk context while outcomes remain influenceable.
- **Evaluate AI through a value lens.** Assess whether governance, workforce readiness, integration and investment discipline are translating AI deployments into measurable improvements in performance, quality, capacity and decision-making.
- **Challenge whether investment follows risk.** Test whether resources, ownership and capability-building align with the exposures leaders identify as most significant, particularly where talent and third-party concerns appear to exceed investment.
- **Modernise internal audit's operating model.** Align talent, technology, data, specialist access and sourcing strategies with the speed, interdependence and technical complexity of the risk environment. Apply to internal audit's own AI initiatives the same expectations for adoption, governance and measurable value that the function expects from the enterprise.

About the survey

Our 15th annual **Executive Perspectives on Top Risks and Opportunities Survey** contains insights from 1,330 board members and C-suite executives (including 152 CAEs) around the world regarding their views on:

- Ability to transform and protect the enterprise and respond to market opportunities and risks;
- Opportunities for growth considering the current environment;
- Priorities perceived as most critical to maximising the value of AI deployments;
- The top risks on the horizon for the near-term (two to three years ahead) related to 30 specific risks across three dimensions (transform, protect and respond);
- A discussion of their organisations' near-term strategic investment priorities, given the opportunities and the risks they face; and
- The long-term horizon based on 11 risk themes that encompass the 30 near-term risk issues.

Our survey participants shared their views through an online survey conducted in June and July 2026.

About the author



Andrew Struthers-Kennedy is Protiviti's Global CAE Solutions Leader, guiding the firm's strategy, innovation and delivery across all internal audit domains – from technology audit and SOX advisory to audit transformation and analytics. With more than two decades 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.

Contact Andrew at andrew.struthers-kennedy@protiviti.com.

Protiviti (www.protiviti.com) is a global consulting firm that helps clients transform and protect their businesses, and respond to planned and unexpected events. Through a network of more than 90 offices in over 25 countries, Protiviti and its independent and locally owned member firms deliver deep expertise and tailored capabilities across technology, artificial intelligence, data, operations, finance, legal, compliance, HR, marketing, digital, risk, and internal audit—enabling organisations to accelerate innovation, navigate risks and safeguard what matters most.

Named to the Fortune 100 Best Companies to Work For® list since 2015, Protiviti Inc. has served more than 80 percent of Fortune 100 and nearly 80 percent of Fortune 500 companies. The firm also works with government agencies and smaller, growing companies, including those looking to go public. Protiviti Inc. is a wholly owned subsidiary of Robert Half (NYSE: RHI).

© 2026 Protiviti Inc. An Equal Opportunity Employer M/F/Disability/Veterans.
Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services. 1026

protiviti®