# RISK in FOCUS

# 2026/ 2027

Hot topics for internal auditors

# CONTENTS



# EXECUTIVE SUMMARY

Cybersecurity was the predominant threat in Risk in Focus 2026-27, with digital disruption and macroeconomic uncertainty forming a closely-grouped second tier (see Risk rankings).

**With cyber-attacks growing in sophistication and velocity, innovative AI products sweeping onto the market, and growing geopolitical conflict and volatility, most would consider these results to be self-evident, but that is not the full story.**

Strategic decision-making, risk assessment, mitigation and governance strategies are being hampered by the speed at which interconnected risks are developing. Digital disruption, for example, increases the risk of data breaches, creates over-dependence on a few US suppliers, operates within an evolving regulatory environment, redraws traditional business structures and reshapes AI-human interaction. Individually, each of these risks presents a major challenge – but their rapid, unpredictable and simultaneous development is unprecedented. As a result, annual risk assessments and audit planning are quickly becoming outdated, and scarce assurance capacity must be allocated dynamically.

Inevitably, businesses are making trade-offs. By downgrading, for example, climate change risk (against the logic of objective data), or shifting attention from human capital at a time when AI is redefining roles, organisations are increasing their exposure to those threats to deal with urgent trends. But moving a topic down the agenda does not mitigate its potential impacts. It could leave organisational blind spots in emerging, complex and traditional risk areas.

CAEs face major obstacles in supporting boards and organisations to achieve their strategic objectives. In many areas, internal audit effort is not matched to the assessed risk (see Risk vs effort). This is particularly true of macroeconomic uncertainty and digital disruption. However, apparent mismatches should be interpreted carefully.

Organisational governance, for instance, has one of the lowest risk rankings but received the fourth-highest level of internal audit effort (see Risk vs internal audit effort). This may reflect the fact that governance is both a risk category and a capability through which other risks are identified, assessed and managed. CAEs should therefore test whether high levels of effort in mature or traditional assurance areas remain proportionate, risk-based and clearly linked to the organisation's current threat landscape, while ensuring that threats with low-risk maturity, underdeveloped governance frameworks and traditionally high stakeholder expectations do not lose second- and third-line support when they need it most.

CAEs are innovating. Many have abandoned inflexible, annual internal audit planning strategies. More regular risk assessments now drive adaptable schedules that juggle regulatory compliance requirements with urgent business assignments. CAEs said that they had increased collaboration across the enterprise, which has become essential for understanding interconnected and fast-moving risks. This has provided the organisation with risk and control foresight precisely when it is needed, while retaining internal audit's independent professional judgement (see IIA's updated Three Lines Model).

Given the velocity of change across interconnected risks, traditional governance models may no longer be fit for purpose. With the support of CAEs, boards are beginning to evolve more dynamic governance models that are responsive to both the risks and opportunities that today's business landscape presents.

BACK NEXT CONTENTS

# EXECUTIVE SUMMARY

## Key Points

- **Digital disruption, new technology and AI** moved from third to second place in this year's survey – 52% said it was a top five risk. The topic saw the biggest rise in internal audit coverage. But CAEs said that governance frameworks, training and assurance efforts lagged AI innovation, creating potential risk blind spots.
- The increased speed, sophistication and impact of cyber-attacks meant that 86% of CAEs said **cybersecurity and data security** was a top five risk. Internal auditors must ensure their high levels of coverage are truly risk-based and well-calibrated to the nature of today's threats.
- **Macroeconomic and geopolitical uncertainty** ranked third – up one place from last year. Yet risk maturity and internal audit effort were low. CAEs spent more assurance time on impacted topics than on this threat directly, but without efforts to build governance capacity organisations remained vulnerable.
- With 39% of CAEs choosing **human capital, diversity, talent management and retention** as a top five risk, it dropped from second to fifth place. It had a low maturity ranking and internal audit effort was not rated as proportionate by many. Some risk reclassification could imply that effort on AI belongs to this category, but CAEs said that they struggled to provide strategic support.
- **Organisational governance and corporate reporting** was the fourth-highest area of internal audit effort despite only 13% of CAEs choosing the topic as a top five risk – down by 7 percentage points from last year. CAEs may be allocating assurance resources partly based on governance and control maturity, reflecting the role of governance as a capability through which other risks are managed as well as a risk category in its own right.

# INTERPRETING THE RESULTS: BLIND SPOTS, ANCHORS AND WHAT "ALIGNMENT" REALLY MEANS

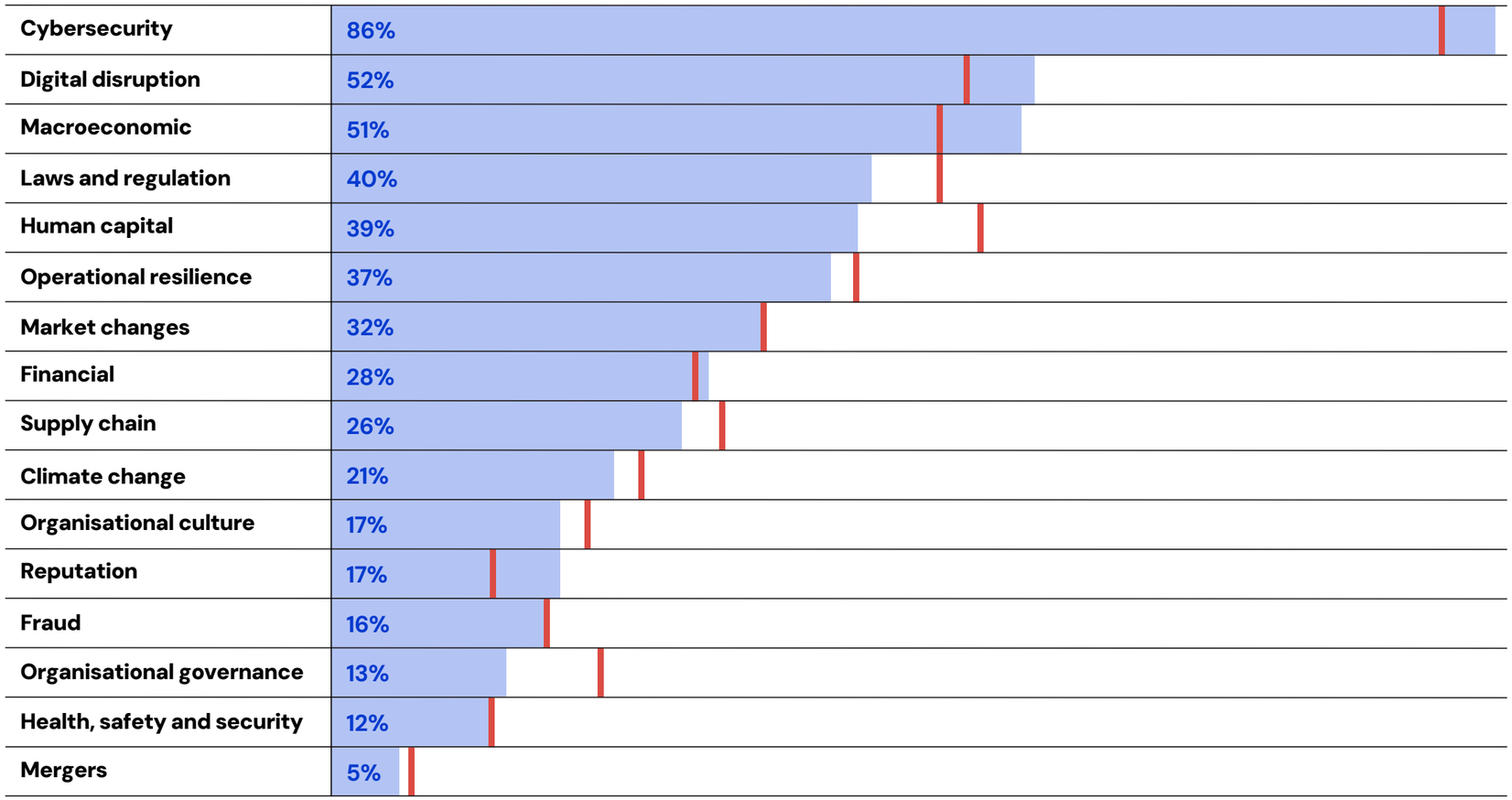
The table brings these themes into sharper focus by summarising each risk's relative position across all seven questions. It enables a side by side comparison of risk exposure (ranking and severity), management capability (maturity) and internal audit response (effort, adequacy, proportionality and intended change).

| | Risk | | | Internal Audit Assurance | | | |
|---|---|---|---|---|---|---|---|
| **Risk** | Rank | Severity | Maturity | Effort | Coverage | Proportionate to risk | Coverage increased |
| Cybersecurity | 1 | 1 | 2 | 1 | 3 | 7 | 2 |
| Digital disruption | 2 | 2 | 16 | 8 | 12 | 15 | 1 |
| Macroeconomic | 3 | 3 | 15 | 15 | 15 | 16 | 12 |
| Laws and Regulation | 4 | 5 | 7 | 2 | 6 | 4 | 5 |
| Human Capital | 5 | 6 | 12 | 9 | 11 | 12 | 8 |
| Operational Resilience | 6 | 4 | 9 | 3 | 5 | 5 | 3 |
| Market Changes | 7 | 7 | 8 | 14 | 14 | 14 | 14 |
| Financial | 8 | 11 | 1 | 5 | 1 | 1 | 10 |
| Supply chain | 9 | 8 | 10 | 7 | 7 | 9 | 4 |
| Climate Change | 10 | 14 | 14 | 12 | 13 | 8 | 11 |
| Organisational culture | 11 | 9 | 13 | 11 | 9 | 11 | 9 |
| Reputation | 12 | 10 | 5 | 13 | 10 | 10 | 16 |
| Fraud | 13 | 13 | 11 | 6 | 4 | 3 | 6 |
| Organisational Governance | 14 | 12 | 4 | 4 | 2 | 2 | 7 |
| Health, safety and security | 15 | 15 | 3 | 10 | 8 | 6 | 13 |
| Mergers | 16 | 16 | 6 | 16 | 16 | 13 | 15 |

This table summarises how CAEs ranked each risk category across the seven survey questions. 1st is the highest-ranked category and 16th the lowest-ranked.

# FINDINGS
## RISK RANKING

Cybersecurity and data security remains the dominant risk.



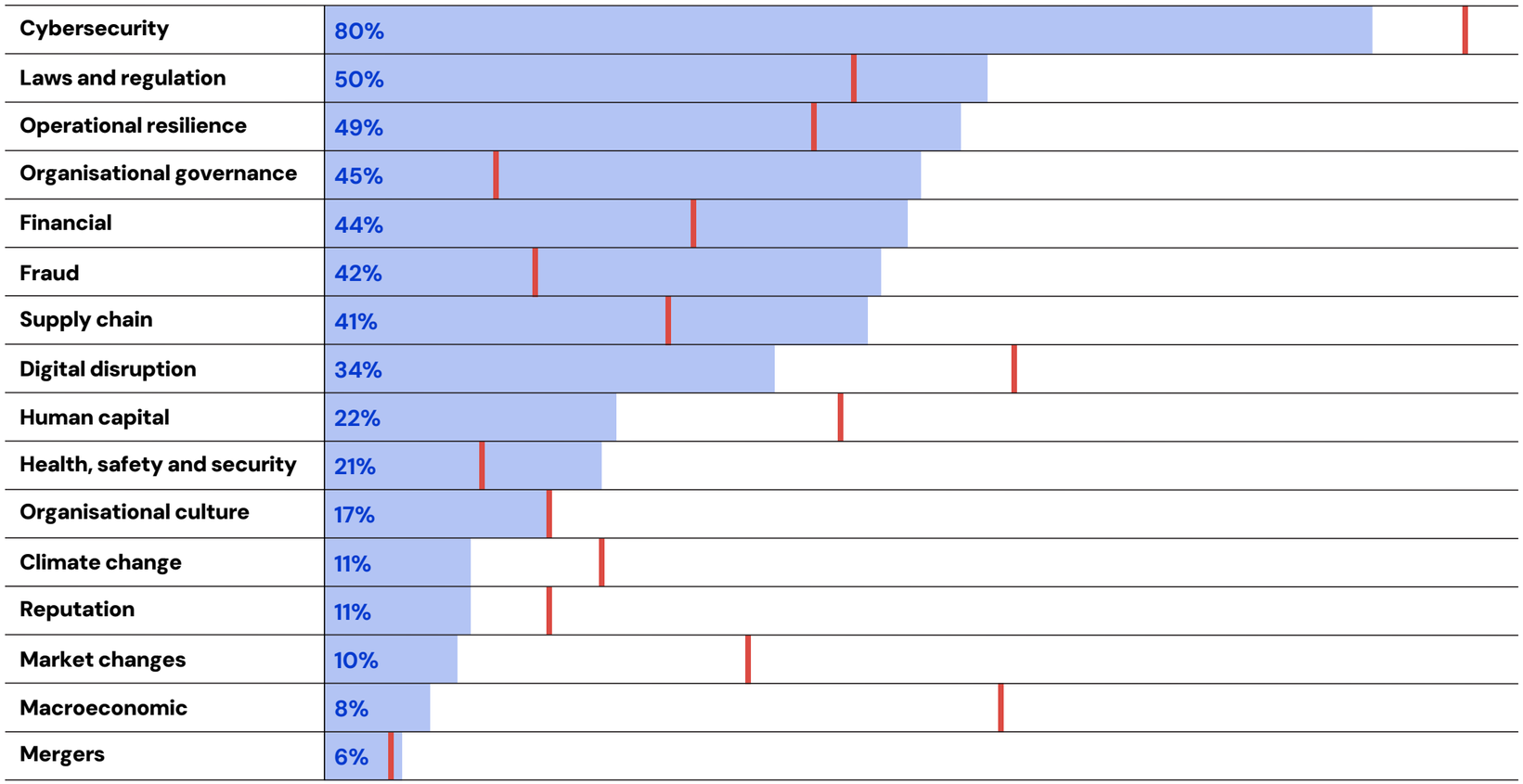

This graph shows the biggest risks faced by organisations across Europe.

BACK NEXT CONTENTS

# FINDINGS

## IA EFFORT COMPARED TO RISK

Cybersecurity is the only area with absolute alignment of the risk ranking and internal audit time and effort – both being first place




This chart shows how CAEs ranked which risk areas they spend the most time and effort.

BACK NEXT CONTENTS

# FINDINGS
## RISK MATURITY

Again, this is a new question introduced this year. It was introduced to enable the analysis to consider risk maturity, ( i.e. the level of sustainable, repeatable and mature enterprise risk management) for each of the 16 risks that they have assessed for importance and severity in their organisation.

| | |
|---|---|
| Financial | 4.16 |
| Cybersecurity | 3.67 |
| Health, safety and security | 3.66 |
| Organisational governance | 3.56 |
| Reputation | 3.56 |
| Mergers | 3.55 |
| Laws and regulation | 3.51 |
| Market changes | 3.41 |
| Operational resilience | 3.37 |
| Supply chain | 3.36 |
| Fraud | 3.34 |
| Human capital | 3.23 |
| Organisational culture | 3.16 |
| Climate change | 3.13 |
| Macroeconomic | 3.11 |
| Digital disruption | 2.87 |

Participants were asked to rank the maturity of each risk with 1 being initial, 2 being infrastructure, 3 being integrated, 4 being managed and 5 being Level 5 optimised. This is the average score for each risk area.

BACK NEXT CONTENTS

# DIGITAL DISRUPTION, NEW TECHNOLOGIES AND AI

## Digital disruption, new technologies and AI

AI is developing at rapid speed. April 2026 alone saw the announcement of four so-called frontier AI models by OpenAI, Anthropic, and Google DeepMind – with Claude Mythos 5 held back because of fears over its ability to hack systemically important banks. European organisations are increasingly implementing AI to capture new opportunities and improve productivity, according to Eurostat.
AI adoption in large enterprises, for example, reached 55% in 2025 – an increase of 14 percentage points from 2024.

Such trends helped digital disruption displace human capital as the second most important risk organisations faced in this year's survey (see Risk vs effort). But both risk maturity and the level of audit coverage were low compared with other topics (see Risk maturity). That suggests that the speed of change in this area requires CAEs to continuously help their organisations to adapt and enhance AI governance frameworks. Those frameworks must take account of both the different levels of AI adoption within the business and remain open to emerging opportunities and risks.

This fast rate of change itself represents a structural feature of technological development, so the potential for risk blind spots to arise is high, including where AI intersects with other threats, such as human capital and cyber security. CAEs must ensure that their audit activities are focused on both building capability in areas such as governance, accountability, model risk and ethics, for example, as well as traditional assurance over controls, as suggested by Risk in Focus 2026-27 interim report.

## Integrating generative AI

Organisations have struggled to manage the adoption of generative AI. A CAE at the roundtable from a technology company in Switzerland said that his organisation's first reaction to the emergence of large language models (LLMs) was to simply block access to popular sites. Introducing a corporate system, which had stronger control environments, mitigated some data security risks. But a CAE at a Spanish utility company said that the cheaply available LLMs staff used at home were often the most powerful – about 34% of professional AI use was unauthorised.


BACK NEXT CONTENTS

# DIGITAL DISRUPTION, NEW TECHNOLOGIES AND AI

CAEs must assess how well the organisation has developed effective strategies to manage such behavioural risks and implemented effective monitoring and controls (see IIA's Organisational behaviour topical requirement).

Once integrated into corporate systems, AI applications can rapidly scan, locate and retrieve documents across an entire enterprise. But access permissions in corporate IT environments were not built to handle these capabilities. CAEs must provide assurance that management has implemented controls to prevent unauthorised access to sensitive data, such as payroll, human resources and even credit card details. In the event of a successful cyber breach that utilised AI models, the consequences could be severe.

But agentic AI makes mitigation control design difficult. "These programs started with simple prompting but now we are moving towards the execution of tasks, which opens up a whole different range of risks," a CAE from an IT business in the Netherlands said. CAEs must consider what it means for an autonomous AI agent to perform tasks as if it were a human team member because that will determine what access permissions such algorithms need, suggesting that a new breed of internal controls and governance rules may be required.

## Balancing the speed of innovation with effective governance

"On a strategic level, balancing the speed of innovation and the risks depends on how much the business is at risk of being disrupted or disintermediated," the CAE from the IT company in the Netherlands said. His business adopted a strong tone at the top to drive fast implementation, redefining its AI risk appetite to cut bureaucracy and create clear boundaries for AI deployment. Those pursuing innovative projects had to complete an AI-enabled risk questionnaire, which automatically categorised projects according to their assessed threat. Only those that were close to breaking the company's threat threshold received a human-led risk assessment.

CAEs said that they were using AI regulations (such as the EU AI Act) to inform the creation of effective governance frameworks. But rapid AI development had disrupted regulatory timetables, creating uncertainty and, perhaps, impacting organisational levels of risk maturity (see Risk maturity). Without well-developed risk governance processes, organisations face blind spots in their coverage of potential threats. In addition, risk management capabilities are likely to lag the high severity of this threat, suggesting that CAEs need to focus on advisory, capability-building and governance-focused approaches rather than pure assurance, according to the Risk in Focus 2026/27 interim report.

Over half of CAEs (57%) said that they had increased audit effort on digital disruption – the largest growth area in the survey (see Audit effort). CAEs at the roundtable said that in providing advisory services on the development of AI governance frameworks they had identified knowledge gaps between key teams. "Organisations need to ensure governance teams and AI project teams are properly connected, grounded together and understand each other to make governance effective," the CAE from the Spanish utility company said.

A CAE at an Austrian financial services firm said that he had conducted a strategic audit on AI for his business. He generally implemented AI assurance reviews within his work on other topics, such as data governance and cybersecurity. This interdisciplinary approach suggests that internal audit support may be higher than reported in the survey. In fact, there were so many interconnected risks associated with AI, a CAE at an Austrian energy company said, that he had carried out a "chain of audits" to provide adequate topical coverage across the enterprise. CAEs need to discuss with relevant stakeholders what adequate coverage means and how that is reflected in a risk-based audit plan.

# DIGITAL DISRUPTION, NEW TECHNOLOGIES AND AI

## AI literacy and decision-making

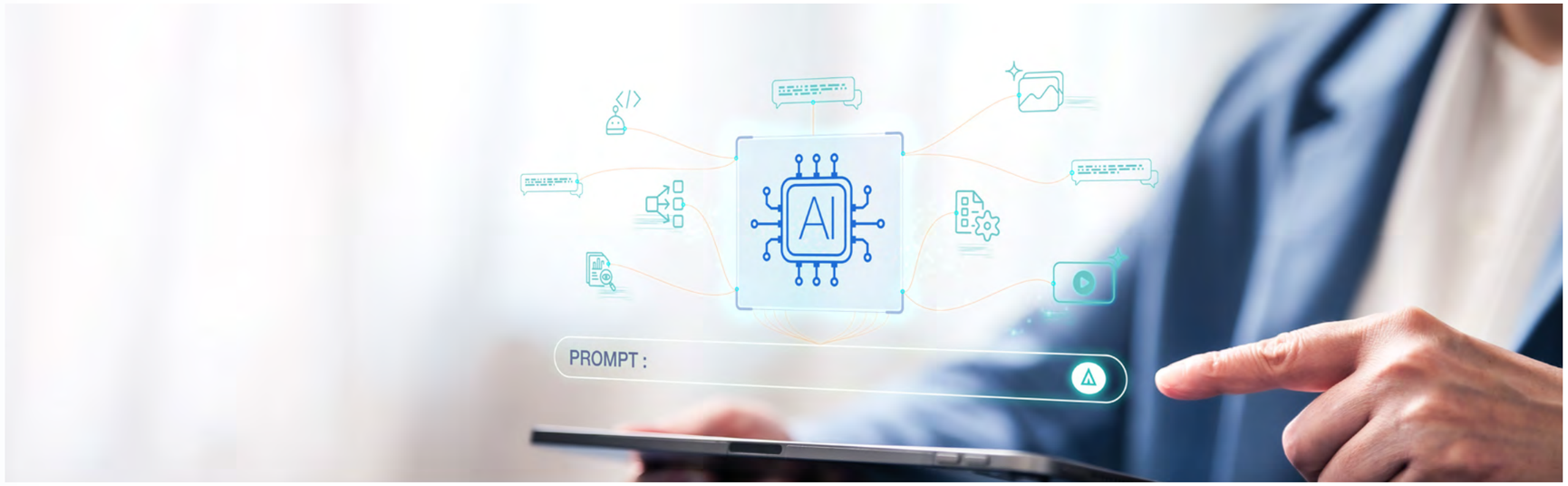
CAEs said there was too much uninformed corporate strategy associated with AI adoption. “The business case, cost-benefit evaluation and risk assessments may be bypassed in the excitement,” the CAE from the technology company in Switzerland said. CAEs should provide assurance that the information underpinning strategic decision-making is accurate and complete so that management can set strategic goals that are realistically costed with appropriate KPIs. CAEs should also assess the need for board and management training on AI and be prepared to engage stakeholders in potentially difficult conversations, according to guidance by IIA Netherlands.

Minimum levels of AI literacy are mandatory under the EU’s AI Act. But CAEs said AI training needed to be properly targeted. Untrained staff could unknowingly create vulnerabilities within the business. “Management must give different levels of access to corporate systems based on AI literacy and the nature of employees’ roles,” the CAE from the Austrian energy business said – a topic suitable for internal audit assurance.

But CAEs must also provide assurance that decisions requiring clear explanation are not left to opaque AI models. “If we cannot explain how we have refused an insurance claim to a judge who does not understand AI, that could be challenging,” the CAE from the financial services firm in Austria said. In this context, internal audit should maintain independent oversight of AI-enabled activities and controls, ensuring that human accountability, effective governance and appropriate challenge remain in place regardless of the degree of automation.

CAEs gave internal audit coverage of AI a low adequacy rating (see Internal audit adequacy). As that coverage increases, the effectiveness of internal audit in an AI-driven environment will depend on the ability of auditors to understand how AI systems operate, identify their limitations and risks, and provide informed, independent assurance and advice on their use across the organisation.

To achieve this, internal auditors will need to develop and maintain the necessary levels of AI knowledge, skills and competencies to effectively evaluate AI-related risks, controls and decision-making processes at a time when the technology is developing at speed.



# DIGITAL DISRUPTION, NEW TECHNOLOGIES AND AI

## CAE action points

1. **Provide assurance that:**

   Data underpinning strategic AI decisions is accurate, complete and robust, and AI goals are realistically costed with appropriate KPIs.

   AI education and training are targeted, linked to controls and competency levels, and available across the organisation, including the board.

   Access permissions, data protection controls and monitoring arrangements are adequate to prevent unauthorised AI-enabled access to sensitive information.

   Strategies, monitoring and controls to manage behavioural risks arising from AI use, including unauthorised use of external AI tools.

2. **Provide advice on:**

   Strengthening AI governance so it reflects different implementation levels, connects governance and project teams, and adapts to emerging risks.

   Whether AI strategy and risk appetite are aligned, balancing commercial opportunities with mitigation, accountability and effective challenge.

   Whether the organisation's governance, access and control frameworks remain appropriate as agentic AI and autonomous tools increasingly execute tasks, make recommendations or interact with corporate systems.

## Other CAE actions

Consider what proportionate AI audit coverage means, and how this should inform a risk-based plan covering governance, accountability, model risk, ethics, decision-making and AI audit skills.

# CYBERSECURITY AND DATA SECURITY

Cybersecurity remained the lead threat in this year's survey with 86% of CAEs choosing it as a top five risk (see Risk rankings).

**AI-generated attacks drove that threat upwards, growing in both quantity and sophistication, leading CAEs at the roundtable to describe it paradoxically as a permanently emerging risk.**

Notable vulnerabilities combined different threat areas, including supply chains, for example, and attacks that used social engineering to bypass authentication systems, according to IBM. CAEs ranked the risk as the most severe threat they faced (see Risk severity). That perception was reflected in real events. For example, a £2 billion cyber incident at the UK manufacturer Jaguar Land Rover had a direct impact on the UK's GDP, according to the Bank of England.

Over half (52%) said that they had increased their coverage of the topic in 2026. It was one of two top five risks where audit effort was closely aligned to the threat – the other being laws and regulations (see Risk vs effort). But CAEs must ensure that efforts are calibrated to current risks and the reliance on the second line and not simply determined by regulation and stakeholder expectations, according to the Risk in focus 2026-27 interim report. High risk maturity in this area and a mediocre score for how proportionate this effort is to the threat suggest that CAEs must ensure that their efforts are truly risk-driven and proportionate to avoid creating potential risk blind spots in other areas.

a **£2 billion cyber incident** at the UK manufacturer Jaguar Land Rover had a **direct impact on the UK's GDP**, according to the Bank of England

## Defending against increased intensity and sophistication

The volume and sophistication of social engineering attacks are increasing. For example, so-called ClickFix attacks deceive users into completing fake verification processes that deploy malware onto corporate systems, a report by Check Point said.

# CYBERSECURITY AND DATA SECURITY

In addition, phishing attacks that imitate key personnel have intensified – a technique reportedly used to create approximately £300 million worth of losses at the British retailer Marks & Spencer. Europol also noted the growth of professional hacking coalitions that aimed to steal data from major technology companies.

"But we can over-emphasise new technological developments from sophisticated and AI-enabled cyberthreats," a non-executive director for several organisations in the Netherlands said. Such attacks tended to exploit vulnerabilities already listed on existing databases, including those maintained by the European Union Agency for Cybersecurity, she said. CAEs should, therefore, provide assurance that patch management processes were effective and that their organisations at least met the minimum level of governance, risk management and controls mandated by IIA's Cybersecurity topical requirement.

Businesses that prioritised implementing AI processes risked straining the resources available to cybersecurity and IT functions. A CAE at a UK financial services firm, for instance, said that introducing AI chatbots into the business had dramatically increased the volume of identity and access approval requests, which management had struggled to validate in a timely manner. That had created delays in routine cybersecurity updates. In addition, to combat the sophistication of social engineering attacks, cybersecurity defence processes needed to consider the threat's connection with human capital. "You can no longer separate cybersecurity from behavioural risk or resilience," she said – underlining the need for CAEs to consider how IIA's Organisational behaviour topical requirement can support their organisations in this area.

## Geopolitical uncertainty complicates risk exposure

The growing entanglement of macroeconomic and geopolitical uncertainty and cybersecurity risk has complicated the threat landscape. For example, unfriendly states are attempting to infiltrate organisations. Some IT freelancers from Singapore applying to work in European businesses, for example, were North Korean nationals, according to Fortune magazine. Anthropic said such workers used its Claude program "to create elaborate false identities with convincing professional backgrounds … and deliver actual technical work once hired." CAEs must provide assurance that human resources departments have upgraded processes and controls to mitigate such risks.

Europe's dependence on US technology for cloud services, AI programs and operational software represents a strategic threat. Vendor lock-in is also a key concern. Without a developed European sovereign cloud industry – only 15% of capacity is based in Europe – few large organisations can achieve strategic autonomy and reduce the possibility of third-country intervention (see Risk in focus 2026 for a discussion). CAEs at the roundtable said that smaller cloud and AI providers may have weaker cybersecurity controls. But the European Union is taking action to increase the number of sovereign cloud providers, and businesses such as aerospace company Airbus are finding ways to locate key strategic data in Europe. CAEs should provide assurance that the board has considered such threats and that the organisation has implemented the governance, risk management and controls recommended by IIA's Third-party topical requirement.

CAEs said that they had limited audit access to US cloud providers, making controls assurance difficult. A provider's own reports on system and organisation controls did not allow for oversight of risk assessment methodologies or tolerances, a CAE at a Spanish telecommunications business said. But collaboration with other internal audit functions could be a solution, a CAE at a large, London-based financial institution said. His organisation pooled resources with other firms to hire a global consultancy to audit their US technology provider. The strategy provided an additional level of assurance but was time-consuming to negotiate and prohibitively expensive for smaller companies.

# CYBERSECURITY AND DATA SECURITY

## Building cyber resilience

"We're moving from a case of not if we get hacked, but when," the CAE from the UK financial services firm said. Her organisation was developing the concept of a minimal viable company to create a more resilient business. She advised the firm on a risk assessment of what systems it would need to have in place to recover from a blackout – from software and buildings to personnel and furniture. When redefining how the organisation needed to categorise its risks based on this strategy, collaboration across the three lines and regular workshops and scenario planning had been especially important, she said. CAEs should collaborate to improve their organisations' ability to anticipate, absorb and adapt to disruption – an approach that closely aligns with IIA's Organisational resilience topical requirement, which comes into force in April 2027.

In fast-moving areas such as cybersecurity, digital disruption and AI, she said that CAEs must constantly discuss, assess and reassess risk categories because annual review processes were no longer adequate to manage either the speed at which risks develop or their interconnected nature. "Businesses must clearly define their strategic, emerging and live risks and make sure everyone knows the difference," she said, "because you'll often see that items on the emerging risk list are actually live." CAEs should discuss with management how taking simple steps, such as putting a timeline on emerging risks and revisiting assumptions once new technologies come online, could improve their assessments.

She had also facilitated risk management workshops for all new technology purchases with the risk owners and the CISO to "find out what could go right and wrong and plan for that." That meant that internal audit was able to provide foresight to inform decision-making, rather than merely capturing what had happened after decisions were made. There is clear evidence in this report that CAEs are supporting boards to create dynamic and forward-looking oversight models to aid decision-making on emerging threats.

The soaring cost of cybersecurity defence has moved up the agenda in boardrooms – as has the need for more proactive, risk-based internal audit support. "Risk management tools must be actively used to manage threats rather than just being used as a retrospective repository of information," the non-executive director from the Netherlands said. Her organisations were considering changes to their risk appetites because of the rising costs of mitigating cybersecurity threats. Strong leadership, company-wide education and firm support at board level were vital to creating effective cyber-resilience, a CAE at a Swiss technology business said. For specific resilience plans, clear recovery time and recovery point objectives were key.

# CYBERSECURITY AND DATA SECURITY

## CAE action points

1. **Provide assurance that:**

   Patch management is timely, risk-based and proportionate to the criticality of the vulnerability and affected systems, and that the organisation meets the minimum governance, risk management and control expectations set out in IIA's Cybersecurity Topical Requirement.

   Human behaviour, social engineering and criminal infiltration risks are identified, evaluated and addressed through appropriate controls.

   Cyber resilience and recovery capabilities are defined, tested and aligned with risk appetite, including recovery objectives and minimum viable operations.

   The pressure AI adoption is placing on cybersecurity and IT control processes, including identity and access approvals, validation activity and routine cybersecurity updates.

   Third-party governance, risk management and controls effectiveness.

2. **Provide advice on:**

   Whether the board has considered strategic technology-provider risks, including cloud concentration, digital sovereignty, vendor lock-in and limited assurance access.

## Other CAE actions

1. Consider collaboration with internal audit functions at other organisations, where appropriate, to increase assurance over strategic third-party service providers and shared technology risks.
2. Use workshops, scenario planning and other forward-looking techniques across the three lines to distinguish strategic, emerging and live risks, test assumptions and support dynamic board oversight across this report.
3. Ensure cyber audit effort is proportionate and calibrated to current risk, risk appetite, second-line reliance and stakeholder expectations, with focus on resilience as well as compliance.

# MACROECONOMIC AND GEOPOLITICAL UNCERTAINTY

About half (51%) of CAEs said macroeconomic uncertainty was a top five risk. But there was a widening misalignment between risk and internal audit effort (see Risk vs audit effort).

**The US and Israel war against Iran, which closed the vital energy route of the Strait of Hormuz, marked the latest chapter in more than six years of macroeconomic and geopolitical volatility. Oil prices peaked at $126 per barrel in 2026 compared with an average price of $69 in 2025 and continued to fluctuate as the conflict stopped and started.**

The crisis provides a perfect example of how a single geopolitical risk event can suddenly trigger a wide range of severe impacts, which are difficult to calculate and manage. The London School of Economics has said that when oil becomes scarce, for example, transport, petrochemicals, fertilisers, manufactured goods, investment capital and energy costs rise. Consumer spending drops, raw material supplies become scarce, while food and power supplies may be rationed. In addition, during the military conflict Iran reportedly launched state-backed cyberattacks against some European businesses.

About half (51%) of CAEs said macroeconomic uncertainty was a top five risk. But there was a widening misalignment between risk and internal audit effort (see Risk vs audit effort). Since 2020, the proportion of CAEs choosing macroeconomic uncertainty as a top five risk has increased by 22 percentage points. But internal audit effort has only increased by 4 percentage points – rising from 4% to 8% in those seven years. Either audit coverage and risk maturity exist within organisations but are focused across the operational categories where the impacts fall, or CAEs are leaving their businesses vulnerable to assurance blind spots.

## Fragility of global trade and supply chain reconfiguration

Forty-one percent of CAEs said that supply chains were a top five risk. A CAE at a European car manufacturer at the roundtable said complexity has strained third-party risk management processes. While his internal audit function had traditionally reviewed sanctions annually as part of its audit plan, he now sought to be more agile, increasing flexibility and focusing on becoming a trusted adviser to the senior board of management.

BACK NEXT CONTENTS

# MACROECONOMIC AND GEOPOLITICAL UNCERTAINTY

Under the Three Lines Model, he said that it was important to ensure internal audit established appropriate access to management and fostered strong lines of communication and collaboration, while retaining independence of judgement. To fully understand the complexity of the risks that the business faced when events moved quickly, he said that he had increased collaboration with management on risk identification and mitigation planning. As a result, he had made a structural shift in his audit-planning strategy. He dropped the yearly planning cycle in favour of reassessing the risk landscape every three months and rewriting the audit plan as needed. Such moves support a finding of this report that boards and CAEs are adopting more dynamic, forward-looking and scenario-based oversight models.

A CAE at a global retailer based in the Netherlands said that he had taken "a layered approach" to specifically deal with macroeconomic uncertainty. First, he questioned management on the risks they faced to assess their severity. Then, based on those discussions, he assessed whether they had in place the right governance frameworks, risk assessment procedures, adequate scenario testing and crisis management processes for their strategic decision-making activities. CAEs should also consider providing an opinion to the board on whether the organisation was able to collect, assess, analyse and act on changes fast enough in a rapidly evolving environment, said the CAE from the Portuguese financial services firm – an area of audit work well supported by IIA's Organisational resilience topical requirement.

"If you look at geopolitical risk as one threat, there is no answer to that," the CAE from the Netherlands said, "so the organisation has to focus on topics such as supply chains, which are tangible." That suggests that CAEs are putting more effort into organisational governance (see below, Organisational governance and corporate reporting), on the one hand, while increasing audit effort most in specific areas that required urgent attention – such as supply chains (see IIA's Third party topical requirement). From that perspective, the survey results may not truly reflect internal audit effort expended on macroeconomic uncertainty, which could be reflected mostly in the impacted risk categories. However, CAEs must ensure that they are still building capability specifically in governance processes that address macroeconomic uncertainty to improve the organisation's risk maturity rating in this area where it is rated as low (see Risk maturity).

## Navigating fragmented and politicised regulation

Macroeconomic uncertainty has increased the complexity of regulatory compliance. Half of survey respondents chose it as a top five area of internal audit effort, second only to cybersecurity – 29% said they had increased the time allocated to the topic in their audit plan (see Audit effort). When war broke out in Iran, for example, a CAE at a Spanish manufacturer said his company had immediately sought to contract new suppliers closer to its factories worldwide. "It was a complex task because the business had to review its components globally, at the same time as assessing any human rights impacts within the supply chain" under the now-revised European Union's Corporate Sustainability Due Diligence Directive (CSDDD), he said.

European and US regulations have recently diverged in areas such as data security and human resources policies. The CAE from the retailer in the Netherlands said that while companies were required to report on diversity under the Corporate Sustainability Reporting Directive (CSRD) in Europe, for instance, "the question of what compliance means is becoming tricky" for companies with dual European and US stock exchange listings. CAEs needed to provide assurance that their organisations were legally compliant in both jurisdictions, he said, at the same time as gauging whether the language on diversity, for example, had been properly considered to meet the needs of both sets of investors.

# MACROECONOMIC AND GEOPOLITICAL UNCERTAINTY

"It would be impossible for internal audit to give assurance that the business is compliant with every single law in every single country," the CAE in the Netherlands added, "but internal audit does have a duty to assess the solidity of the legal processes that oversee those risks, for example, and whether it can be confident that those responsibilities are carried out at a global, regional and local level – as well as by the relevant second line functions." Where internal audit effort is high, CAEs should assess whether assurance responsibilities have been properly allocated in accordance with IIA's Three Lines Model.

## Liquidity in a downturn

CAEs said that it was important never to drop internal audit focus on financial liquidity. In the survey, the severity of this risk was low, while risk maturity was the highest of all topics (see Severity and Risk maturity). It had the best level of coverage, and audit effort was closely aligned with risk (see Risk vs effort). "Macroeconomic downturns are not a risk, they are a certainty," the CAE from the retailer in the Netherlands said, "so, for me, focus in this area is very close to hygiene for the internal audit function."

CAEs must assess the robustness of the governance, risk management and controls over treasury, hedging and financing, he said. In addition, internal audit functions should make sure their rotational audits in these areas are rigorously followed and provide assurance that the basic financing structure of the business and its hedging and treasury policies were up to date and followed. During an economic downturn, the risk of management attempting to circumvent controls to increase profitability and hit targets rose dramatically and would require additional focus, he said.

# MACROECONOMIC AND GEOPOLITICAL UNCERTAINTY

## CAE action points

1. **Provide assurance that:**

   Treasury, hedging and financing are robust, current, consistently followed and resilient during downturns.

   Supply chain and third-party risk processes are agile enough to respond to geopolitical disruption, sanctions, supplier change and due diligence obligations.

   The organisation can identify, assess and act on rapid change, and is building governance capability for macroeconomic uncertainty.

2. **Provide advice on:**

   Whether strategic decision-making processes appropriately consider short-, medium- and long-term macroeconomic and geopolitical risks, including relevant assumptions, trade-offs and crisis management arrangements.

   Whether legal, sanctions and regulatory compliance processes are sufficiently robust across global, regional and local levels, including whether responsibilities are clearly allocated to relevant second-line functions.

## Other CAE actions

1. Communicate and collaborate closely with management and risk holders to improve risk identification, mitigation planning and access to timely insight, while retaining internal audit's independence of judgement.
2. In areas where audit effort is high, assess whether assurance responsibilities are clearly assigned and effective across the organisation, and whether assurance activities are appropriately coordinated under the Three Lines Model to identify gaps, duplication and opportunities for reliance.

# HUMAN CAPITAL, DIVERSITY, TALENT MANAGEMENT AND RETENTION

This year's Risk in focus survey found that only 39% of CAEs said it was a top five risk compared with 48% in 2025.

BACK NEXT CONTENTS

**When the European Commission launched its recommendations for boosting skills in November 2025, it said that "the tallest mountain ahead of the EU is the persistent shortage of workers and specialised skills."**

The topic dropped from second place to fifth place in the risk rankings – the largest fall of any (see Risk rankings). Internal auditors were also deprioritising work in this area: effort dropped by five percentage points to 22%, and it ranked poorly for proportionality, adequacy and risk maturity – suggesting that more focus was needed.

The results are puzzling. Prior to the COVID-19 pandemic, risk and audit effort were relatively well aligned (Risk in focus 2020). While the risk ranking rose rapidly during and after the pandemic, internal audit effort has remained roughly at 2020 levels. That has created one of the largest misalignments in the survey (see Risk vs effort).

Explanations are speculative. First, some risk displacement may have occurred as CAEs re-categorise certain human capital risks as belonging to digital disruption, AI and cybersecurity. That trend is reflected in the themes chosen by CAEs at the roundtable for this chapter, which deals mostly with AI-related strategies. But it could also indicate that boards have deprioritised the threat despite the objective risk it poses to the company – an issue CAEs should raise with the appropriate stakeholders. Second, CAEs participating in Risk in focus over the past few years have noted a lack of internal audit knowledge and skills in areas where the primary risks are often not suitable for traditional assurance assignments (see, for example, Risk in focus 2024). This suggests that internal audit's response may be failing to keep pace with organisational needs. CAEs should assess how far human capital governance processes are being disrupted by AI – exposing businesses to serious blind spots in this area.

## AI-driven job disruption and deskilling

How AI will change skills, roles and staffing needs is an open question. For example, the research body IPPR estimated that up to eight million jobs could disappear in the UK, but AI may also boost GDP and create new roles. The reality for organisations is likely to be a mixture of those two trends.

# HUMAN CAPITAL, DIVERSITY, TALENT MANAGEMENT AND RETENTION

CAEs at this year's roundtable on the topic said that these potential impacts were already influencing how management reported the outcomes of the initial assessments of AI. "People may be reluctant to share a strategy that shows potential free time created by AI and they are thinking about how to reclassify this time differently," a CAE at an Italian manufacturer said. As a result, CAEs should provide assurance that their businesses have the right control processes in place to mitigate patterns of behaviour that may undermine human capital objectives in line with IIA's Organisational behaviour topical requirement.

CAEs at the roundtable said that management was frequently resistant to internal audit support in this area. A CAE at a fashion company in Spain said she had added an advisory project focusing on how AI was affecting roles in her organisation to a planned assurance assignment on HR policies. Under what she called a "hybrid arrangement," the scope, objectives and responsibilities of the two parts of the exercise had to be clearly explained to the auditee under the IIA's revised Global Internal Audit Standards. But she said that management had been keen to consider the findings of her advisory work, opening the door to similar projects.

## Challenges and strategies in AI adoption

CAEs were more confident this year that their organisations had got to grips with AI programs and processes (see Risk in focus 2026 for issues with the early implementation of generative AI). But CAEs must support the board so that it has an accurate, timely and balanced view of the impact of AI-human interactions on future staffing needs and the design of new roles. With 59% of organisations interpreting AI through a technology lens, according to a report by Deloitte, too few boards were making progress in restructuring traditional organisational functions. In fact, human resource departments may lack the necessary skills and insight to assess such developments, so collaboration or merger with the relevant IT functions could be key to capturing the upsides of digital transformation at a strategic level.

The CAE at the Spanish fashion business said that it was vital to provide assurance around both AI-human processes within the business and the relevant governance structures. "If there is no proper governance, that will create risks around human and automated decision-making processes, including the ethics associated with AI," she said. With regulatory compliance deadlines approaching under the EU's AI Act, CAEs should facilitate workshops in areas where it will be critical to understand, for example, whether decisions within algorithmic recruitment processes are "fair" and whether a human or an AI agent is making critical decisions.

CAEs said that internal audit functions that had implemented AI could use that experience to better support the adoption of the technology within their organisations. For example, direct experience with AI could improve the identification of current and emerging risks, help with planning for future skills, as well as assist with choosing topics (such as AI-human collaboration) to include in internal audit plans. For internal audit functions, research by Chartered IIA shows that embracing AI is likely to lead to the automation of lower-value work and a greater focus on strategic topics and risk assessments. CAEs should assess whether time saved through AI automation in the business is strategically redeployed to higher-value activities such as innovation, employee development and risk management.

## Talent management and skills realignment

CAEs said that areas of focus included training, reskilling, upskilling and assessing the organisation's future talent requirements. "We have developed a quality matrix for AI talent management to aid decision-making for the board and the C-suite," a CAE from a Swedish financial services firm said. This had also

# HUMAN CAPITAL, DIVERSITY, TALENT MANAGEMENT AND RETENTION

helped to measure the company's ambition for AI adoption and provided a clear roadmap for achieving the right skills at a higher level across the enterprise.

Building the governance framework had been a collaborative process with the business, IT and human resources departments with internal audit acting in an independent advisory capacity. It was vital that the governance framework in this area was flexible enough to both adapt to the different levels of AI readiness in the organisation and to capture possible future trends, she said. That had meant developing two parallel systems to deal with each of those factors within the governance process. She had facilitated detailed scenario planning exercises to assess the emerging skills landscape and plan for the organisation's projected skills needs in line with its business strategy. Boards must evolve towards such forward-looking, scenario-based oversight models if they are to adapt to an increasingly dynamic environment.

A CAE at an insurance company in the Netherlands had prepared a series of readiness reviews to help the board in this area. That involved helping management create an inventory of future skills that focused on its AI strategy and business goals. The company decided to recruit based on the skills needed to support the strategy of the enterprise rather than on individual departmental needs – a growing trend.

Soft skills, such as critical thinking and ethics, emerged as crucial topics for organisations – especially in high-risk areas that may require a human to remain in the loop alongside AI decision-making. In addition, collaborative working and the rapid sharing of new skills were proving to be more important than simply having expertise segmented into specific job functions. Organisations that fail to consider how changing human resources trends impact their business models expose themselves to significant risk blind spots.


BACK NEXT CONTENTS

# HUMAN CAPITAL, DIVERSITY, TALENT MANAGEMENT AND RETENTION

## CAE action points

1. **Provide assurance that:**

   Controls mitigate behaviours that may undermine human capital goals, including undisclosed AI-created capacity, role impacts or skills implications.

2. **Provide advice on:**

   How far AI is disrupting human capital governance processes, including whether responsibilities, controls and escalation routes remain clear across HR, IT, risk and business leadership teams.

   Whether time saved through AI-enabled automation is strategically redeployed toward higher-value activities, including innovation, employee development, risk management and enhanced internal audit advisory support.

   Whether human capital is appropriately prioritised in risk assessment, board agendas and audit plans where skills shortages, retention or AI workforce disruption remain material.

## Other CAE actions

1. Support the board so that it has an accurate, timely and balanced view of the impact of AI-human interaction on future staffing needs, role design, skills requirements and organisational restructuring.
2. Assess whether AI-enabled recruitment, workforce planning and decision-making processes are fair, ethical, explainable and subject to appropriate human oversight and challenge.
3. Collaborate with the enterprise in an advisory capacity to develop flexible, forward-looking AI-human capital governance processes, future skills inventories and readiness reviews aligned to AI strategy and wider business goals.
4. Where management is reluctant to engage with internal audit, consider adding clearly scoped advisory dimensions to planned human capital assurance engagements to increase constructive dialogue on emerging workforce risks.

# ORGANISATIONAL GOVERNANCE AND CORPORATE REPORTING

Organisational governance and corporate reporting represented the fourth highest area of internal audit effort despite only 13% of CAEs choosing the topic as a top five risk – down by 7 percentage points from last year (see Risk vs effort).

**Internal audit coverage continued to increase. CAEs said that risk maturity was high; internal audit coverage and proportionality were both the second highest in the survey (see Risk maturity and proportionality).**

So just how does a low-risk topic attract such high internal audit effort compared with emerging risks, such as digital disruption and macroeconomic and geopolitical uncertainty, where risk maturity is low?

This apparent misalignment of risk and effort has existed since the topic was first introduced in Risk in focus 2021. CAEs could be expending too much effort on traditional assurance areas using tried and tested methodologies rather than tailoring their strategies to take account of how assurance categories have been disrupted by interconnected risks that are transforming rapidly, according to the Risk in focus 2026/27 interim report. However, organisational governance is both a risk category and a capability through which other risks are identified, assessed and managed, providing a potential reason for internal audit's high level of effort.

## Board effectiveness and decision quality under complexity

Boards have become more effective, say researchers at Harvard University. Around 70% of global executives trusted their boards to steer them through a crisis; 35% said they were doing a good job. A traditional aspect of board effectiveness is how well they make decisions while considering the current threats and opportunities their organisations face. But with risks transforming at speed, decision-making assumptions are more vulnerable to error – suggesting that boards need support to adopt more dynamic, forward-looking oversight models.

"Most internal audit assurance still provides hindsight because it looks back at how management has designed controls, how those have been implemented and embedded," a CAE at a construction company in the Netherlands said at the roundtable. "We try to provide foresight through our advisory engagements." He had increased the number of informal conversations with management to identify any potential risk blind spots, while discussing with the board where threats were likely to remain unidentified and overlooked in the audit plan.

BACK NEXT CONTENTS

# ORGANISATIONAL GOVERNANCE AND CORPORATE REPORTING

In practice, that had entailed facilitating risk workshops to understand management's perception of its risks, to bring fresh perspectives, offer challenge – and to learn. For example, management and the board tended to steer discussions towards risks with high-probability impacts. But he urged them to also consider the impacts of lower-probability risks if those threats accelerated. "The theme of velocity complicates the discussion and provides risk owners with a different perspective to consider," he said.

Not all organisational governance structures permit such flexibility. A CAE from a government agency in Austria, for example, said that he was unable to directly audit executive decision-making processes because he reported directly to the CEO and CFO. A CAE from a financial firm in Spain said that while auditing the board's activities, assurance work was limited to analysing historical actions and discussions – reducing the opportunity for foresight. "We are less able to challenge them with alternative scenarios, understand the trade-offs they have made, or to provide them with some genuine debate," she said. The function had extended its work to review the outcome of board decisions and to provide feedback on the quality of those choices.

While heavily regulated industries had substantial assurance duties in traditional risk areas, CAEs were providing strategic insights where possible. "As well as providing advisory services, we have been attaching a short document to each standard audit report called 'strategic fields'," the CAE from Spain said. Those reports prompt management to consider the implications of internal audit's assurance findings for the organisation's strategy.

CAEs must innovate to provide such insight, especially in areas such as macroeconomic uncertainty and digital disruption, because European companies often lack committees dedicated to those topics, according to Ecoda. Where organisations have established such committees, they often do not require auditing, nor are there specific advisory assignments needed, a CAE from a French IT company said. But CAEs still have a role: "Informally, I find myself acting as a bridge between process owners, the traditional operations of the company and these ad hoc governance teams to help them explore, for example, how they need to adapt as AI goes from project mode to becoming the everyday reality of the company." Understanding how such risks could impact the organisation's business model, its governance structures and strategies was a vital component of those discussions, she said.

## Internal audit's evolving role in governance and advisory

"Stakeholders want us to be part of the governance of the company, so every internal audit function has to find a sweet spot based on the resources available to it," the CAE at the construction business in the Netherlands said. One approach was to allocate assurance resources to topics based on the maturity of the control frameworks across the organisation. Where risk and governance maturity was high, audit automation technologies could help CAEs expand the proportion of time in their audit plan available for advisory work.

But trends such as AI are disrupting existing control frameworks. "There are more topics requiring you to update your governance and your business models, so that a process-control perspective becomes less relevant," the Netherlands-based CAE said. Ongoing changes to European regulation had contributed to making "governance frameworks very unstable," he said. In addition, extra assurance must be provided to ensure that cultural, ethical and governance processes align, according to reports by Global IIA and IIA France. Taken together, these factors may help to explain the persistence of high internal audit effort on operational governance, suggesting that some CAEs may be spending a proportionate amount of time on the issue, but rating the risk level too low.

# ORGANISATIONAL GOVERNANCE AND CORPORATE REPORTING

## Governance of emerging and interconnected risks

CAEs were increasingly focusing on the interconnectivity between risks – a trend that has grown in this project since the pandemic of 2020. "It is utopian to believe you can look at risks in isolation," the CAE at an IT business in the Netherlands said.

The CAE from the French IT business said she had allocated a greater proportion of the audit plan to "transversal audits." The function took a process or risk and examined it across several countries or business operations. That entailed reducing coverage of traditional areas at a regional level to capture how, for example, an AI control weakness in a peripheral area of the business could have a large impact on its global operations.

CAEs said that they could not determine the materiality of some risks without help. "It is not a discussion internal auditors can have alone," said the CAE at the IT business in the Netherlands, "you really need to sit down with management and help them think through at a higher level what the broader consequences of control failings may be." For example, opening a retail store in a new market that was not financially significant at present still needed to reflect the organisation's cultural standards to maintain brand consistency and reputation.

Communicating the magnitude of interconnected risks was particularly challenging. The CAE from the French IT business said that she had been thinking of adding a compound risk score for topics to help with audit planning. While the enterprise risk management framework only helped her to score risks individually, she was looking at ways to combine those individual results to help her prioritise her assurance work. "Our perception of the audit space would be a starting point," she said, "but then we would use management as a sounding board and, where we found strong correlation, we could devise a plan to provide assurance on the compound risk." Such initiatives reinforce a finding from the qualitative data that many CAEs are seeking to increase collaboration with the business to better understand the risks the organisation faces while retaining their independence.

BACK NEXT CONTENTS

# ORGANISATIONAL GOVERNANCE AND CORPORATE REPORTING

## CAE action points

1. **Provide assurance that:**

   Governance, information and decision-making processes underpin strategic choices.

2. **Provide advice on:**

   Cultural, ethical and governance processes remain aligned as emerging risks disrupt control frameworks and operating models.

   Whether existing governance processes adequately reflect the impact of emerging and interconnected risks, such as AI, geopolitical uncertainty and regulatory change, on the governance model itself.

   How and what constructive feedback on decision quality, outcomes, assumptions and trade-offs could be provided where possible.


## Other CAE actions

1. Test whether governance audit effort remains proportionate, risk-based and linked to the current threat landscape, including governance's role as an enabling capability.
2. Use governance and control maturity, alongside risk severity and velocity, to inform assurance allocation and identify where audit automation could release capacity for higher-value advisory work.
3. Act as an independent bridge, where appropriate, between process owners, traditional operations and ad hoc governance teams to help the organisation understand how emerging risks affect business models, governance structures and strategy.
4. Represent interconnected and compound risks proportionately in the audit plan, using management input and compound risk scoring where this improves prioritisation.

# APPENDIX I - METHODOLOGY

The findings in this report are based on a UK and European survey of Chief Audit Executives (CAEs). The survey was open from 2 March to 7 April and attracted 797 completed responses from across Europe. Responses covered a broad mix of countries, sectors and organisation sizes.

Respondents were asked to assess the following:

- The top risks facing their organisation
- The severity of those risks
- The maturity of their organisation's risk management in each area
- The time and effort internal audit devotes to each area
- The adequacy and proportionality of current audit coverage
- Whether internal audit coverage has increased, decreased or remained stable over time

# APPENDIX II - RISK CATEGORIES

| | |
|---|---|
| **1. Climate change, biodiversity and environmental sustainability** | Climate impacts, resource scarcity, biodiversity loss and tightening environmental regulations affecting operations and strategy. |
| **2. Cybersecurity and data security** | Cyberattacks, ransomware, data breaches and identity compromise undermining digital security and trust. |
| **3. Digital disruption, new technologies and AI** | Rapid technological change, AI adoption risks, system failures and technology driven market disruption. |
| **4. Financial, liquidity and insolvency** | Macroeconomic volatility, inflation, market instability and cash flow pressures heightening insolvency risk. |
| **5. Fraud, bribery and criminal exploitation of disruption** | Fraud, corruption, financial crime and opportunistic exploitation during periods of instability or crisis. |
| **6. Health, safety and security** | Physical harm, security threats, well-being risks and unsafe operating conditions, including geopolitical instability. |
| **7. Human capital, diversity, talent management and retention** | Labour market shortages, demographic trends, skills gaps and evolving cultural expectations affecting workforce stability. |
| **8. Macroeconomic, social and geopolitical uncertainty** | Political conflict, sanctions, social unrest and global economic shocks influencing organisational exposure. |
| **9. Market changes, competition and evolving consumer behaviour** | Shifting customer demand, competitive disruption, innovation cycles and rapid market transformation. |
| **10. Mergers and acquisitions** | Financial transaction and legal risks, valuation uncertainty, integration challenges and post deal instability impacting performance. |
| **11. New and changing laws and regulations** | New or evolving legal requirements, regulatory expectations or jurisdictional divergence are creating compliance pressure. |
| **12. Operational resilience, crisis management, business continuity and disaster response** | Disruptive shocks such as cyberattacks, natural hazards, supply chain failures or infrastructure outages affecting operational stability. |
| **13. Organisational culture** | Misconduct, leadership failures, poor behaviour and cultural resistance creating organisational vulnerability. |
| **14. Organisational governance and corporate reporting** | Governance failures, ethical breaches, reporting inaccuracies and rising transparency expectations. |
| **15. Reputation, communication and stakeholder relationship** | Public criticism, media pressure, misinformation or regulatory scrutiny that damages trust and organisational reputation. |
| **16. Supply chain, outsourcing and nth party risk** | Supplier failures, geopolitical constraints, logistics disruption and weaknesses across extended third party ecosystems. |

# APPENDIX III - SURVEY QUESTIONS

1. Please select and rank the top 5 risks your organisation is currently facing (1st being the biggest risk)
2. Please rate the severity of the following risks for your organisation in 2026/27.
3. For each risk category, please rate the level of risk maturity at your organisation.
    - Level 1 – Initial, e.g. ad hoc and unstructured governance
    - Level 2 – Infrastructure, e.g. has structures in place, but not much beyond the mechanics of a process
    - Level 3 – Integrated, e.g. co-ordinated across the organisation with good interaction
    - Level 4 – Managed, e.g. Very good reporting and use of dashboards for risk-based decision making
    - Level 5 – Optimised, e.g. Fully embedded and transparent with excellent professionally challenging discussions and variety of views fully explored before decisions are made for the benefit of the organisation.
    - Don't know
4. Please rank the top 5 risk areas on which internal audit currently spends the most time and effort (1st being the risk where most time is spent)
5. How would you rate the adequacy of internal audit's current coverage across the following risk areas? (1 being inadequate coverage and 7 being full and adequate coverage.)
6. How confident are you that internal audit coverage across the listed risk areas is proportionate to the risks your organisation is facing? (1 being not confident, 7 being very confident.)
7. In comparison to your 25/26 internal audit plan has your 26/27 internal audit plan coverage increased, decreased or stayed the same?

# ABOUT RISK IN FOCUS

For the past 11 years, Risk in Focus has sought to highlight key risk areas to help internal auditors prepare their independent risk assessment work, annual planning and audit scoping. It helps Chief Audit Executives (CAEs) to understand how their peers view today's risk landscape as they prepare their forthcoming audit plans for the year ahead.

This year, Risk in Focus 2026 involved a collaboration between 13 European Institutes of Internal Auditors, spanning 14 countries including Austria, Belgium, France, Germany, Greece, Hungary, Ireland, Italy, The Netherlands, Norway, Spain, Sweden, Switzerland and the UK.

The survey elicited 797 responses from CAEs across Europe. Simultaneously, five roundtable discussions were organised with CAEs on each of the risk areas covered in the report.

IIA Austria

Institute of Internal Auditors Belgium

IFACI IIA France

DIIR Deutsches Institut für Interne Revision e.V.

Institute of Internal Auditors Greece

The Institute of Internal Auditors Hungary

Associazione Italiana Internal Auditors

The Institute of Internal Auditors Netherlands

The Institute of Internal Auditors Norway

Instituto de Auditores Internos de España

IIA Sweden

The Institute of Internal Auditors Switzerland

Chartered Institute of Internal Auditors

ECIIA