
RISK in FOCUS
2026/ 2027
Hot topics for internal auditors
BOARD BRIEFING

RISK IN FOCUS 2026/27
EXECUTIVE SUMMARY

- Strategic decision-making, risk assessment, mitigation and governance strategies are being hampered by the speed at which interconnected risks are developing.
- As boards increase the time allocated to urgent trends, they risk deprioritising threats such as human capital and climate change; moving a topic down the agenda does not mitigate its potential impacts and may create organisational blind spots.
- CAEs are innovating to support boards and management by moving away from inflexible annual audit planning, increasing collaboration across the enterprise and using advisory work to provide risk and control foresight while retaining internal audit's independent professional judgement.
- With the support of CAEs, boards are beginning to develop more dynamic governance models that are responsive to both the risks and opportunities that today's business landscape presents.

← BACK NEXT →

RISK IN FOCUS 2026/27 HOT TOPICS

- **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 (see Key survey findings for complete risk ranking data, page 4). 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 with 51% of CAEs choosing it as a top five risk. Yet risk maturity and internal audit effort remained low. CAEs spent more assurance time on affected topics than on this threat directly, but without efforts to build governance capacity, organisations remain vulnerable.

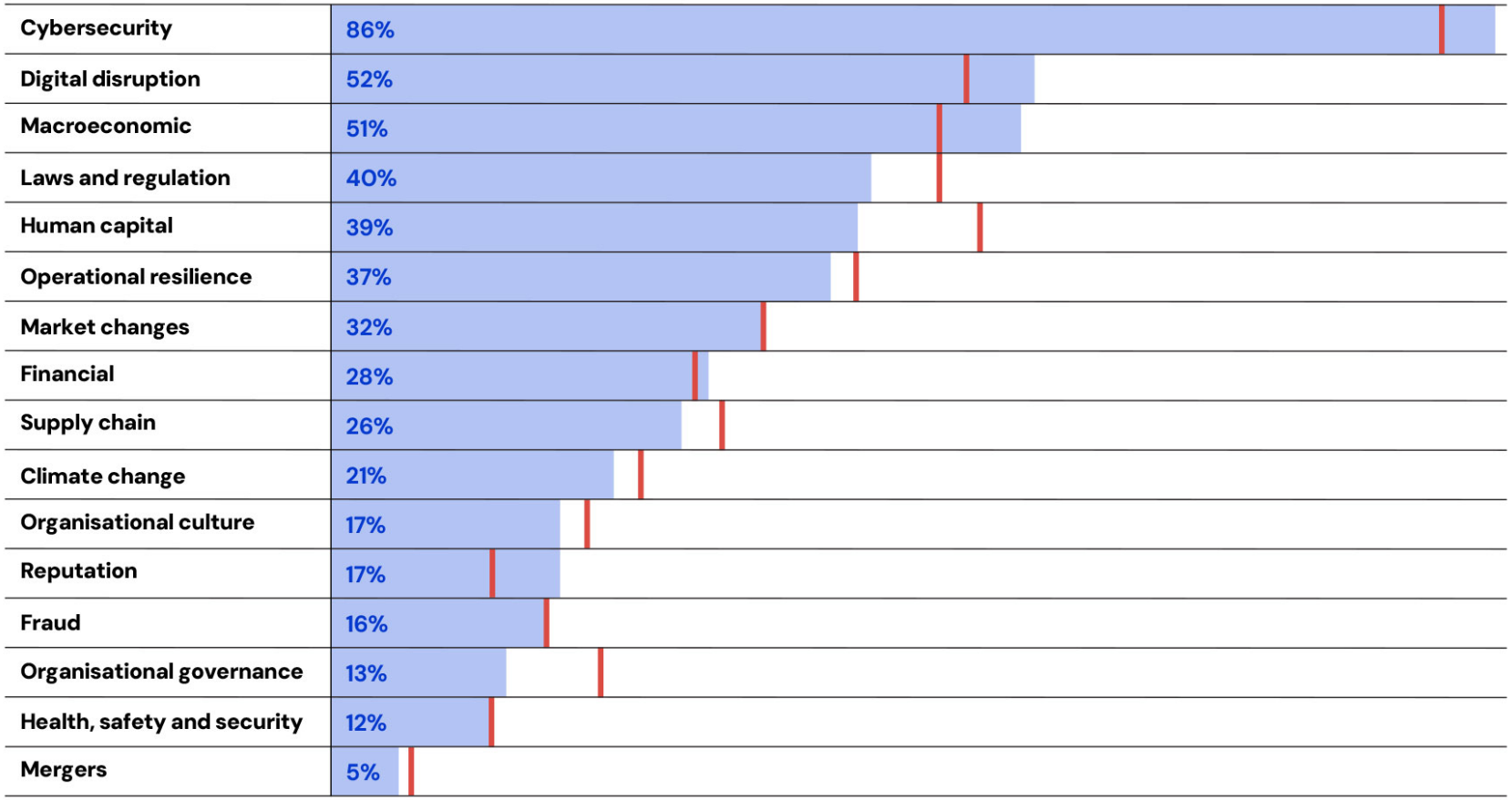
- With 39% of CAEs choosing **human capital, diversity, talent management and retention** as a top five risk, it dropped from second to fifth place – below **new and changing laws and regulations** (40%) in fourth place. It had a low risk maturity ranking and internal audit effort was not rated as proportionate by many. Some risk reclassification may imply that effort on AI belongs to this category, but CAEs said they struggled to provide strategic support.

- While only 13% of CAEs chose **organisational governance and corporate reporting** as a top five risk, CAEs said it was the fourth-highest area for internal audit effort. This may reflect the role of governance as both a risk category and an enabling capability through which other risks are identified, assessed and managed.

← BACK NEXT →

FINDINGS
RISK RANKING

Cybersecurity and data security remains the dominant risk.



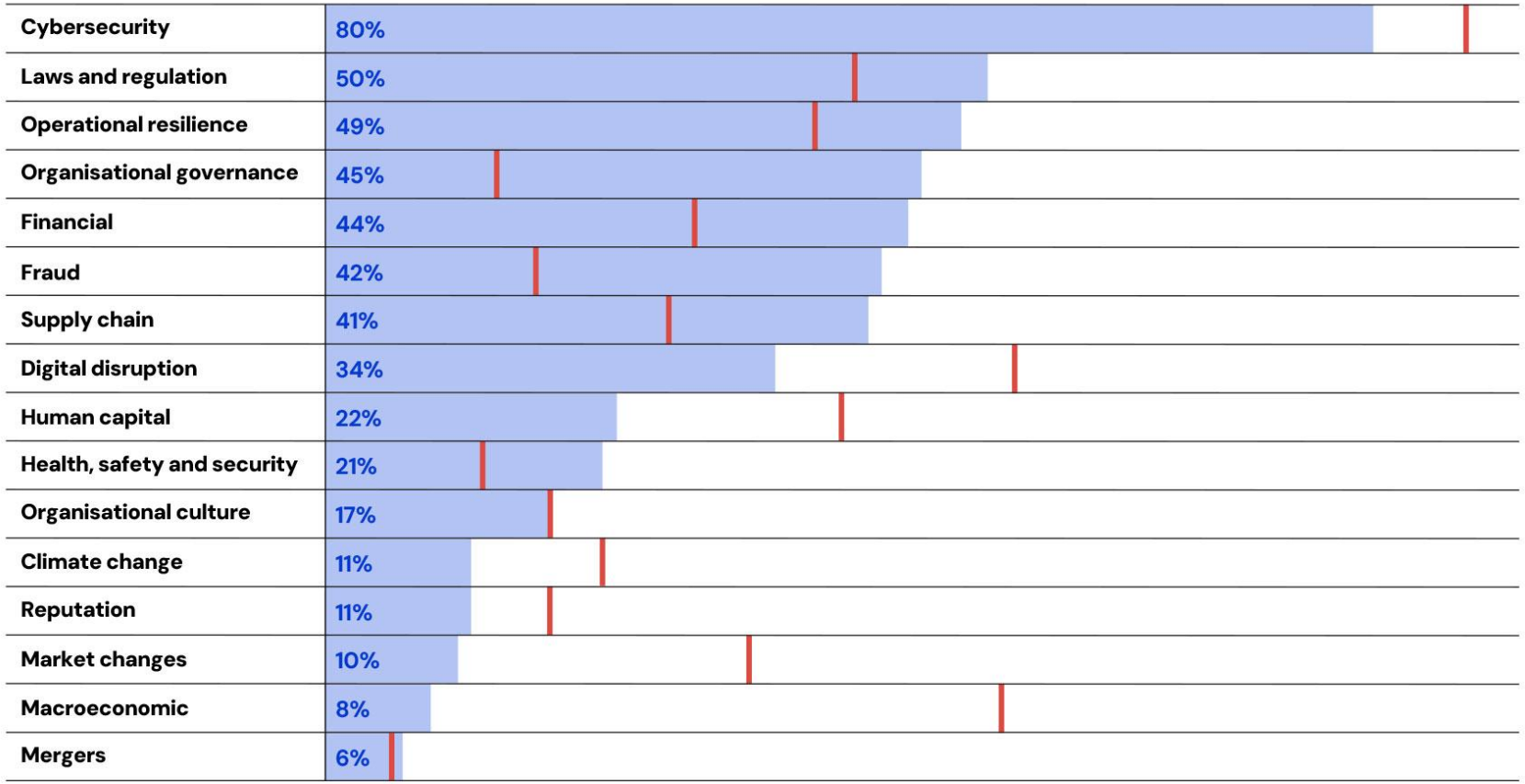
This graph shows the biggest risks faced by organisations across Europe.

← BACK NEXT →

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 →

DIGITAL DISRUPTION, NEW TECHNOLOGIES AND AI: KEY FINDINGS

"On a strategic level, balancing the speed of innovation and the threats depends on how much the business is at risk of being disrupted or disintermediated."

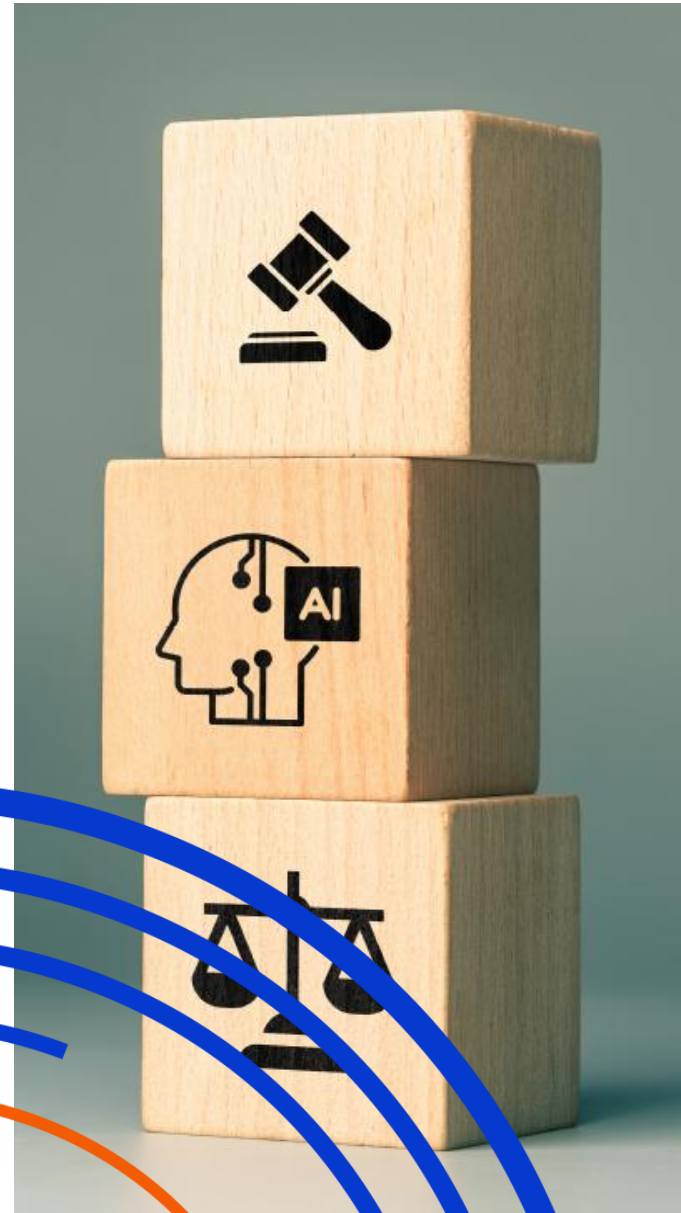
- Digital disruption displaced human capital as the second most important risk organisations faced in this year's survey – 52% said it was a top five risk. But risk maturity and internal audit coverage were comparatively low, suggesting that governance, assurance and capability-building activity have not kept pace with AI innovation.
- The velocity of change represents a structural feature of AI development, increasing the potential for risk blind spots, especially where AI intersects with other threats, such as human capital and cybersecurity.
- Organisations were struggling to adapt internal controls and governance processes to deal with agentic AI. Many were assessing the impact of autonomous agents on IT systems and traditional operational functions.
- Improving AI literacy across the enterprise was a key focus as algorithmic decision-making becomes embedded in operational systems, and boards need assurance that accountability, explainability and effective challenge remain in place regardless of the degree of automation.

BACK NEXT

DIGITAL DISRUPTION, NEW TECHNOLOGIES AND AI: KEY BOARD CONSIDERATIONS

"The business case, cost-benefit evaluation and risk assessments may be bypassed in the excitement."

- How well is the organisation's AI strategy aligned with its risk appetite, and are commercial threats and opportunities balanced with appropriate risk mitigation?
- Do the organisation's AI governance frameworks and structures take account of different levels of AI implementation across the business, and are they adaptable to emerging risks?
- Are educational programmes on AI well-targeted, linked to risk controls and competency levels, and available at all levels of the business?
- Has the board discussed with the CAE whether the proposed risk-based internal audit coverage is appropriate, including whether sufficient attention is given to capability building in areas such as governance, accountability, model risk and ethics?



BACK NEXT

CYBERSECURITY AND DATA SECURITY:
KEY FINDINGS

"We're moving from a case of not if we get hacked, but when."

- Cybersecurity remained the lead threat with 86% of CAEs choosing it as a top five risk. AI-generated attacks drove that threat upwards, growing in both quantity and sophistication, but CAEs must ensure that high levels of coverage remain risk-driven, proportionate and calibrated to current threats.
- Businesses that prioritised implementing AI processes risked straining the resources available to cybersecurity and IT functions, creating delays to essential risk mitigation processes.
- European organisations faced increasing strategic threats from over-reliance on US hyperscale businesses for both cloud and AI applications, leading some organisations to seek to locate key digital assets within Europe's growing sovereign data industry.
- The soaring cost of cybersecurity defence has increased demand for proactive, risk-based internal audit support focused on cyber resilience, recovery capability and the organisation's ability to anticipate, absorb and adapt to disruption.

← BACK NEXT →

CYBERSECURITY AND DATA SECURITY:
KEY BOARD CONSIDERATIONS

"You can no longer separate cybersecurity from behavioural risk or resilience."

- How well are cybersecurity vulnerabilities that overlap with human resources, such as employee behaviour and criminal infiltration, identified, evaluated and addressed through appropriate controls?
- Has the board considered its dependence on US hyperscale businesses for strategic data and AI applications, and assessed whether concentration risk could be mitigated by moving some data to European sovereign providers?
- Has the board implemented a dynamic oversight model for cybersecurity to ensure that regular workshops and scenario planning properly categorise and mitigate interconnected risks and capture emerging developments?
- How far does the organisation's assurance work on cybersecurity, risk management and controls build the organisation's resilience capabilities?

← BACK NEXT →

MACROECONOMIC AND GEOPOLITICAL UNCERTAINTY: KEY FINDINGS

"If you look at geopolitical risk as one threat, there is no answer to that."

- Macroeconomic and geopolitical uncertainty ranked third in 2026-27 – up one place from last year. Yet risk maturity was low and there was a widening misalignment between assessed risk and internal audit effort, raising the possibility that assurance activity is focused on impacted operational categories rather than the threat itself.
- Supply chains were a major area of focus – 26% of CAEs said they were a top five risk. The complexity of interconnected risks led to an increased level of communication and collaboration between management and assurance providers.
- Macroeconomic uncertainty increased the difficulty of regulatory compliance and underlined the need for robust governance, risk management and controls over treasury, hedging and financing.
- CAEs were restructuring their internal audit planning systems. Some had exchanged annual audit planning for more flexible, agile models that reassess the risk landscape more frequently and adjust assurance activity as conditions change.

← BACK NEXT →

MACROECONOMIC AND GEOPOLITICAL UNCERTAINTY: KEY BOARD CONSIDERATIONS

"Macroeconomic downturns are not a risk, they are a certainty."

- How well does the organisation maintain a clear focus on its financial liquidity and the robustness of the governance, risk management and controls over treasury, hedging and financing?
- How far do decision-making processes appropriately consider short-, medium- and long-term risks, including relevant scenarios, assumptions and trade-offs?
- Does the board receive appropriate assurance from the CAE on whether the organisation has effective processes to collect, assess, analyse and escalate significant strategic and operational changes in a timely manner?
- How far are the frequency of the internal audit planning processes and the nature of audit activity tailored to support the board's ability to manage emerging risks associated with macroeconomic uncertainty and other topics undergoing rapid change?

← BACK NEXT →

HUMAN CAPITAL, DIVERSITY, TALENT MANAGEMENT AND RETENTION: KEY FINDINGS

"If there is no proper governance, that will create risks around human and automated decision-making processes, including the ethics associated with AI."

- Only 39% of CAEs said human capital was a top five risk compared with 48% last year. Internal audit effort also fell. CAEs at a roundtable held on the topic for this report said that this decrease may reflect risk displacement or reclassification into digital disruption, AI and cybersecurity rather than a genuine reduction in exposure.
- Organisations were working to redesign roles and operational functions based on the changes inherent in AI-human interactions, although too many boards viewed digital transformation through a purely technological lens, potentially limiting their return on investment.
- Businesses were creating future skills inventories and shifting towards skills-based workforce planning, with some organisations focusing on the capabilities needed to support enterprise strategy rather than on traditional departmental headcount alone.
- As AI decision-making becomes more prevalent in recruitment practices, organisations are strengthening their controls in light of regulatory requirements.

← BACK NEXT →

HUMAN CAPITAL, DIVERSITY, TALENT MANAGEMENT AND RETENTION: KEY BOARD CONSIDERATIONS

"We have developed a quality matrix for AI talent management to aid decision-making for the board and the C-suite."

- How far has the organisation implemented governance, risk management and control processes in its initial assessments of the impact of AI on the workforce to mitigate patterns of behaviour that may undermine human capital objectives?
- How well do governance processes around human resources activities reflect the distinction between AI and human decision-making, retain critical human judgement where needed, and align with regulatory requirements?
- Have the board and management developed forward-looking tools and processes to assess emerging skills needs and operational restructuring strategies in an AI-human workplace?
- How far has the board integrated its digital transformation and organisational transformation strategies to capture the upsides of emerging human-AI capabilities?

BACK NEXT

ORGANISATIONAL GOVERNANCE AND CORPORATE REPORTING: KEY FINDINGS

“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.”

- While only 13% of CAEs chose organisational governance and corporate reporting as a top five risk, CAEs said it was the fourth-highest area of internal audit effort. This apparent misalignment may reflect governance’s role as an enabling capability through which other risks are identified, assessed and managed.
- With threats transforming at speed, decision-making assumptions are more vulnerable to error, suggesting that boards need support to adopt more dynamic, forward-looking oversight models.
- CAEs were increasingly allocating assurance resources according to governance and control maturity as well as risk severity. But fast-moving trends such as macroeconomic uncertainty, AI and regulatory change can destabilise existing control frameworks and make traditional process-control assurance less effective.
- Organisations were seeking to calculate the materiality of interconnected risks by collaborating across the three lines and experimenting with compound risk scores.

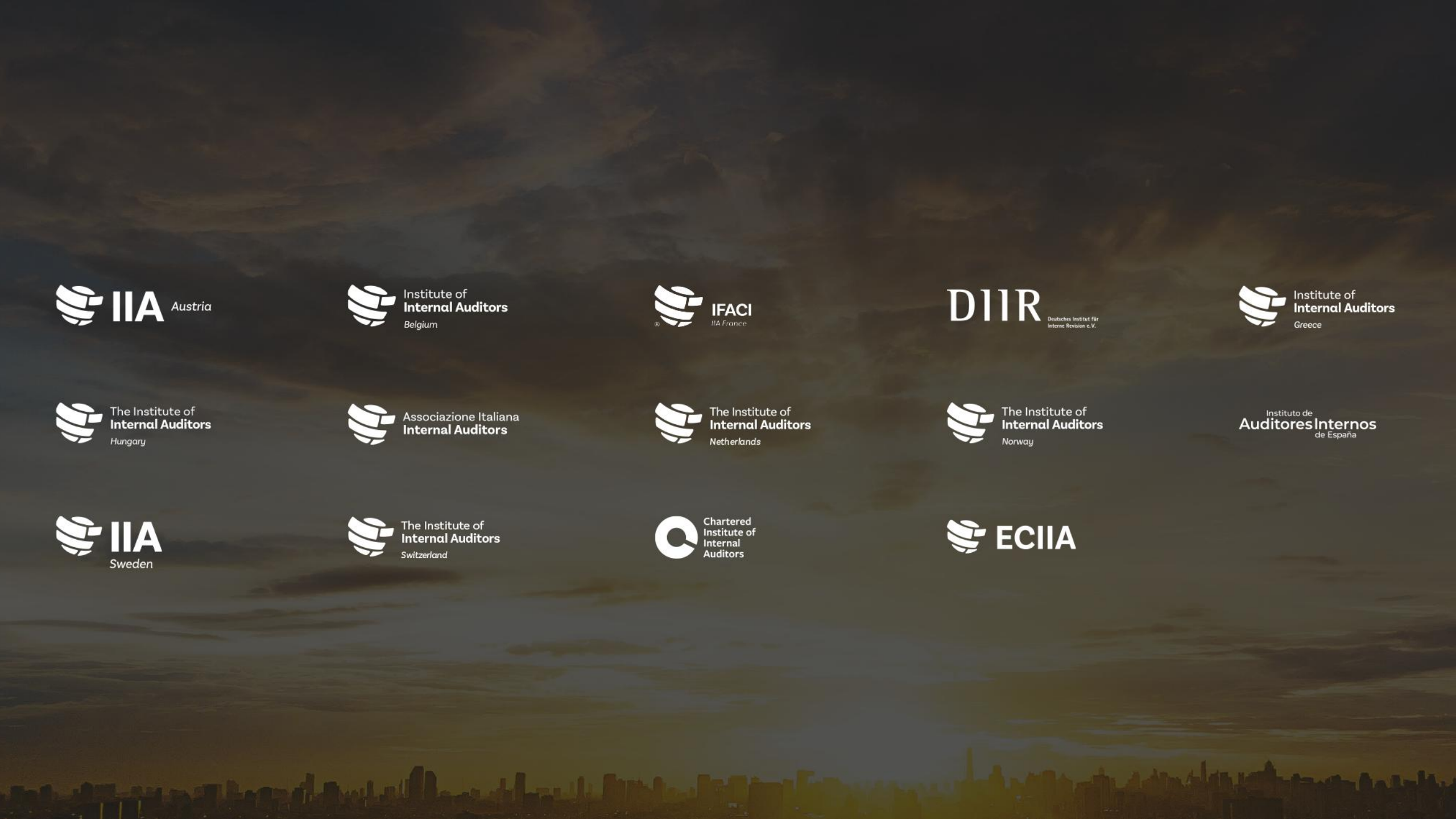
← BACK NEXT →

ORGANISATIONAL GOVERNANCE AND CORPORATE REPORTING: KEY BOARD CONSIDERATIONS

"The theme of velocity complicates the discussion and provides risk owners with a different perspective to consider."

- How far has the organisation considered 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 do the board and management ensure that governance, information and decision-making processes underpinning strategic choices are well-designed, based on timely information and able to identify potential risk blind spots?
- How far do the board and management consider the impact of potentially low-impact risks where they may interact with other threats, and how might the velocity at which risks crystallise alter their impact?
- How well does the CAE support the board by providing foresight on key risks, challenging assumptions and providing insight and advice on the adequacy of dynamic, forward-looking oversight models?

BACK NEXT


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