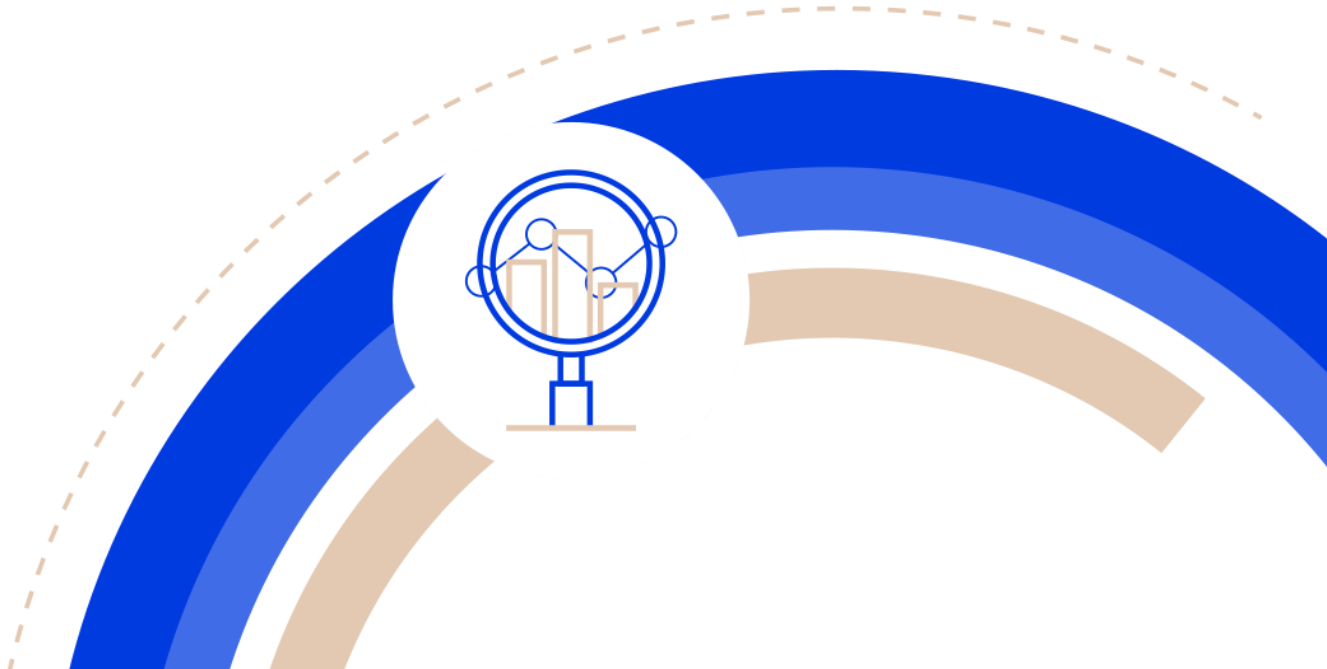

2025
RISK IN FOCUS
Hot topics for internal auditors
BOARD BRIEFING
Read more
ECIIA

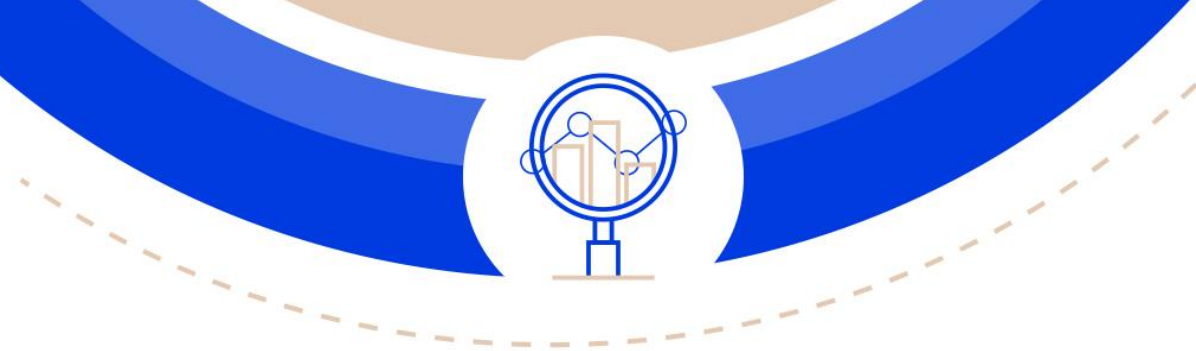
RISK IN FOCUS 2025
EXECUTIVE SUMMARY

- Organisations are rushing to adopt new technologies to gain competitive advantage in a volatile and fast-moving risk landscape.
- An iron-clad focus on strategy, risk management and skills will be key to success.
- While Europe's economy is expected to grow during 2025, its businesses face fierce headwinds powered by a mixture of political uncertainty, climate risk, regulatory pressure and changing demographic trends among the workforce.
- But the prevalent driver for 2025 is digital disruption. The newest generation of artificial intelligence (AI) tools have made competition and market demands a key strategic focus – and a huge risk.



RISK IN FOCUS 2025

HOT TOPICS



- **Digital disruption, new technology and artificial intelligence (AI)** was the survey's fastest riser – going from 6th place in 2024, to 4th place in 2025 and expected to rise to 2nd position by 2028.

- Deep fake attacks and increasingly intense AI-powered hacks helped **cybersecurity and data security** retain its long-standing position as the top threat with 83% saying it was a top 5 risk. A special question on the negative impact of AI on organisations identified rising threats from cybersecurity and fraud as the biggest risks.

- For the third year running, **human capital, diversity, talent management and retention** held its 2nd place ranking with 52% of CAEs placing it as a top 5 risk. Balancing shifting demographic trends with skills and budgetary shortages at a time of increased digitalisation is a challenge.

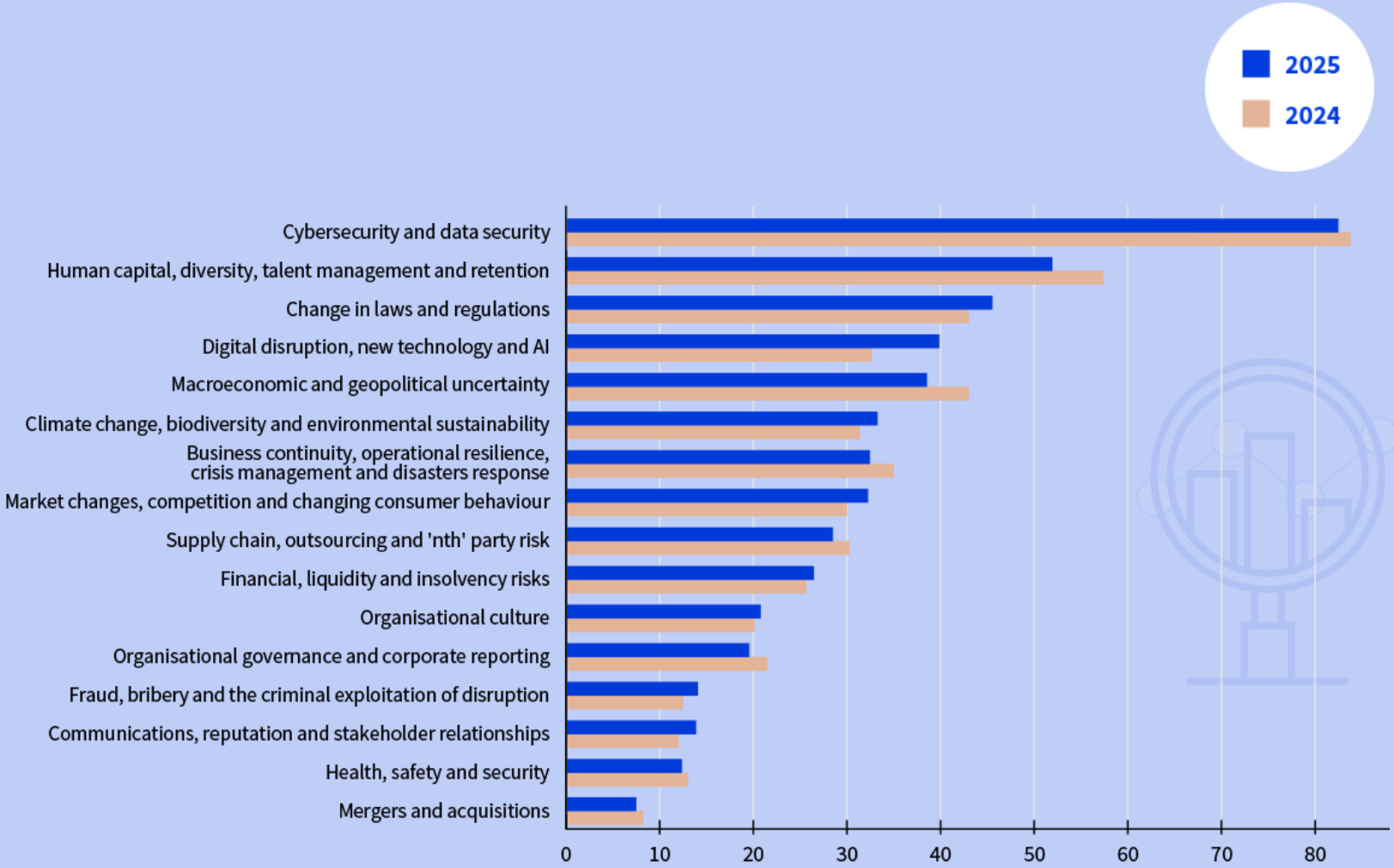
- **Macroeconomic and geopolitical uncertainty** lost its 3rd place ranking to changes to laws and regulations, dropping to 5th in 2025, with 39% of CAEs identifying it as a top five risk. Grey zone aggression – the ability of state and state-sponsored actors to disrupt operations and trade – emerged as a major concern, along with the use of deepfake technologies to influence political developments

- **Climate change, biodiversity and environmental sustainability** ranked 6th with 33% saying it was a top five risk. Increasing regulatory pressure from incoming rules under, for example, Europe's Corporate Social Responsibility Directive is expected to push it to 4th place by 2028.

Key survey findings

The top 5 risks organisations face today

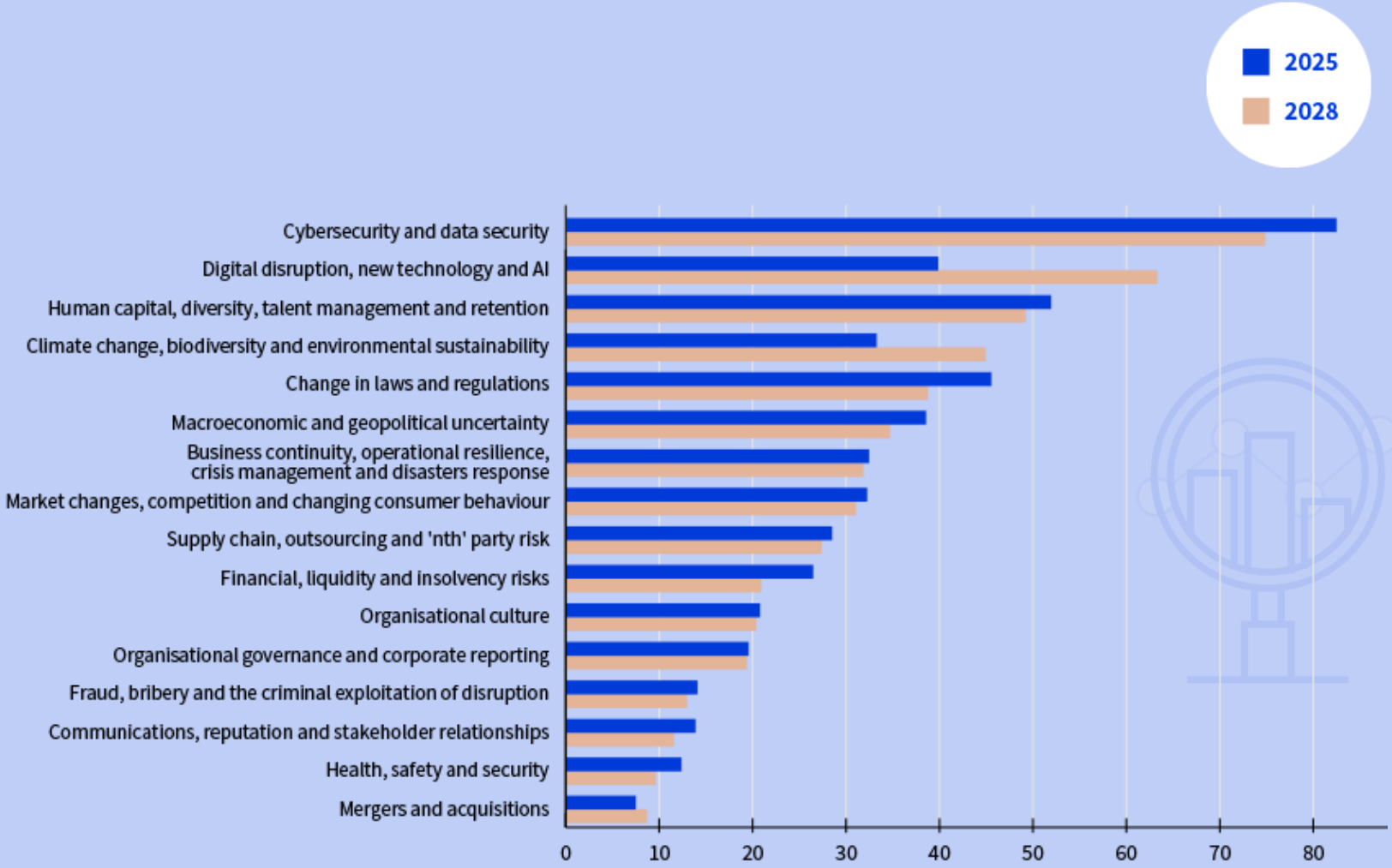
Digital disruption, new technologies and AI was the fastest rising category. Organisations are under intense pressure to ramp up efforts to meet growing market demands and keep up with competitors.



Looking ahead

The top 5 risks organisations will face by 2028

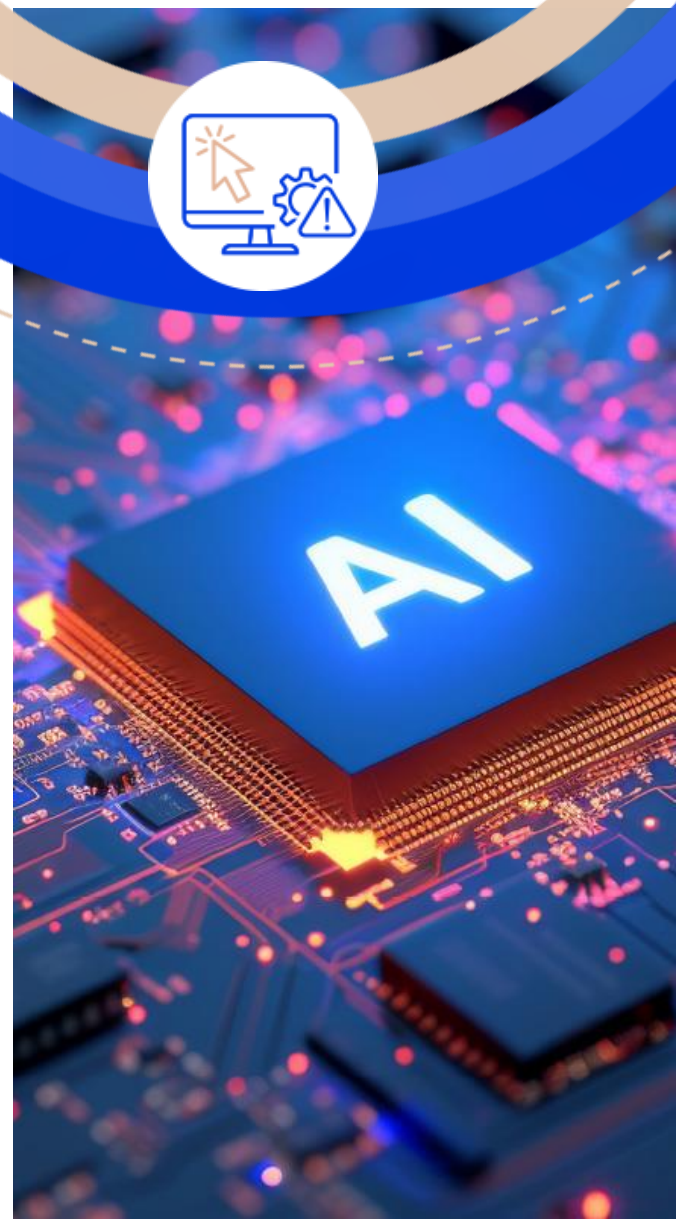
Technology risks will dominate the rankings by 2028 with climate change risk becoming a top 5 risk. The persistence of people risk suggests organisations may struggle to attract, develop and retain the right talent to meet these challenges.



DIGITAL DISRUPTION, NEW TECHNOLOGY AND ARTIFICIAL INTELLIGENCE: KEY FINDINGS

"Digitalisation was often piecemeal and divorced from the strategic objectives of their organisations"

- Digital disruption, new technology and artificial intelligence was the fastest rising risk category in this year's survey. It was predicted to rise from 4th to 2nd place by 2028. Together with cyber and data security, technology will dominate the risk landscape.
- But many organisations had fragmented digital and AI strategies with little centralisation or control over innovation.
- The European Union's AI Act had provided a framework for risk assessment, but it contains vague risk categories. In addition, practices differed over what type of ethical approach to take over AI.
- AI specific skills were in short supply and recruitment policies and practices still needed better alignment with AI strategies.



DIGITAL DISRUPTION, NEW TECHNOLOGY AND ARTIFICIAL INTELLIGENCE:
KEY BOARD CONSIDERATIONS

"If organisations do not have AI in their strategy, they will not be successful in the future"

- Does the organisation have a specific AI strategy and appropriate governance framework as required by the EU AI Act, and are risks and opportunities properly identified – including in 3rd party suppliers?
- How far are AI efforts centralised to avoid fragmentation and are they supported by AI governance policies and guidelines?
- Are the business' recruitment practices and procedures tightly aligned to the organisation's AI strategy and are they effective in helping the business to acquire and develop critical skills?
- Is the organisation's stance on ethics in relation to AI clear and transparent?

CYBERSECURITY AND DATA SECURITY:
KEY FINDINGS

"The more sophisticated the attack, the greater the concern. That is why people are becoming a more crucial part of our defences than ever"

- Cybersecurity and data security remained the top risk for businesses with the volume and velocity of attacks rising rapidly because of new artificial intelligence (AI) hacking techniques.
- In addition, deepfake methods rose seeing hackers impersonate key personnel. At some organisations, hackers had used fake ID to gain physical access to systems – blurring the distinction between internal and external threats for cyber-defence professionals.
- Organisations were strengthening resilience through compliance readiness programmes aimed at implementing new cyber-related regulations (DORA and NIS2).
- Strengthening awareness of cyber and data security across organisations was a major focus in addition to using AI to boost automated defences.

CYBERSECURITY AND DATA SECURITY:
KEY BOARD CONSIDERATIONS

"Audits are crucial, but dialogue with IT management and executive management to ensure they focus on these areas, share information across the business and raise awareness is also fundamental if you want to become resilient"

- Is the board actively engaged with cybersecurity and data security as required by the NIS2 directive and how does that engagement manifest itself in practical terms?
- How well are cybersecurity and data security efforts coordinated across the enterprise – including in emerging areas such as deepfake hacking – and how well is the organisation adopting cutting-edge AI to automate defences where possible?
- Are third-party partners' cyber and data controls adequate, transparent and reliable given that the board's members potentially have personal liability for poor controls across the value chain (under NIS2) – and does the definition of such partners take account of how they must be understood by, for example, regulation such as the Corporate Sustainability Reporting Directive?
- Is cyber and data security culture across the enterprise healthy and do staff at every level engage with the process?

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

"It is likely that people will cycle through organisations more often than they used to because they are looking for different things"

- Human capital issues retained their 2nd place ranking in this year's survey and will continue to be a top five risk by 2028 with organisations struggling to adapt their cultures to the shifting needs and values of multigenerational workforces.
- Human resources recruitment and retention processes often lacked transparency or the agility to cope with high staff turnover. Greater rates of attrition among key talent centred around internal barriers to promotion.
- Staff disengagement was a persistent issue, especially where the recommendations of employee surveys remained unimplemented.
- Digitalising human resources departments continued to lag in many businesses because of the slow take up of new technologies and distrust in artificial intelligence.

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

"Areas such as strategic workforce planning have become so complex that whatever plan we come up with, it will almost certainly be wrong. But there must be a clear direction of travel around which the organisation can flex"

- How involved is the board in supporting initiatives within the business to adapt the organisation to the needs and values of a multigenerational workforce?
- How clear and transparent is the organisation's messaging on its core values, policies and ambitions both inside and outside the business?
- Given the importance of increased digitalisation, how well is human resources integrated into those efforts and could the better use of artificial intelligence improve recruitment and retention initiatives?
- How well does the board understand the interdependencies between succession planning, inclusion, diversity, ESG and culture in strategic decision making?

MACROECONOMIC AND GEOPOLITICAL UNCERTAINTY: KEY FINDINGS

"Only companies that have a vision of where the world is going are likely to survive"

- Macroeconomic and geopolitical uncertainty was a top 5 risk for organisations this year, with state-actors and small countries raising the stakes in disruptive physical and cyberattacks that fell short of actual warfare.
- Regulations, trade embargoes and sanctions were ongoing and unpredictable with several high-profile businesses suddenly banned from supplying key customers outside of Europe.
- General elections in Europe and across the globe added extra uncertainty around inflation, tax and climate-related regulation.
- Many organisations were working to better integrate risk assessments into strategic decision making and focusing on stress testing, scenario planning and disaster recovery.

MACROECONOMIC AND GEOPOLITICAL UNCERTAINTY:
KEY BOARD CONSIDERATIONS

"In a volatile world, resilience [is about] how fit your business model is, and how robust your governance processes are"

- How far does the organisation's approach to risk management capture the impact of threats across the entire business and from its entire supply chain rather than only from the perspective of individual sections and functions?
- Do enterprise risk management processes feed into the board's strategic decision making and are those decision-making processes properly supported by stress tests and scenario planning exercises?
- Is there adequate challenge to assumptions on risks and opportunities in the board's decision-making processes and how well are diverse voices represented?
- How effectively is the board kept up to date on emerging risks and are the potential impacts of those risks' on the strategic goals of the organisation properly understood?

CLIMATE CHANGE, BIODIVERSITY AND ENVIRONMENTAL SUSTAINABILITY:
KEY FINDINGS

"Issues such as extreme heat and the availability of water can effectively put you out of business"

- Climate change was one of the fastest-rising risks this year, driven by regulatory compliance, physical risk and transition efforts.
- Bringing data accuracy up to the same level as that used for financial reporting was a key challenge, with some organisations struggling to meet annual reporting deadlines.
- Since Europe is the fastest-warming continent globally, organisations have boosted investment in technologies to protect physical assets and improve future resilience.
- Many businesses did not have clear targets and metrics around their transition plans making it difficult to identify and take advantage of new business and investment opportunities.

CLIMATE CHANGE, BIODIVERSITY AND ENVIRONMENTAL SUSTAINABILITY:
KEY BOARD CONSIDERATIONS

"We are focusing on operational resilience planning and creating contingency plans under a range of scenarios so we will be able to respond to most circumstances in the future"

- What assurance is there that the organisation's climate-related data is as accurate as that used for financial reporting and that public statements are backed by solid data to avoid the risk of greenwashing or litigation from stakeholders against the company and its directors?
- Does the organisation have plans in place to manage any possible impact of late reporting on investor relations and reputation?
- How far does the organisation use technologies to manage physical assets and how well is the business future-proofed against extreme weather?
- Do the business' net zero transition plans have concrete metrics and targets and are they flexible enough to quickly take advantage of emerging opportunities?