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

CONTENTS

Contents

EXECUTIVE SUMMARY:

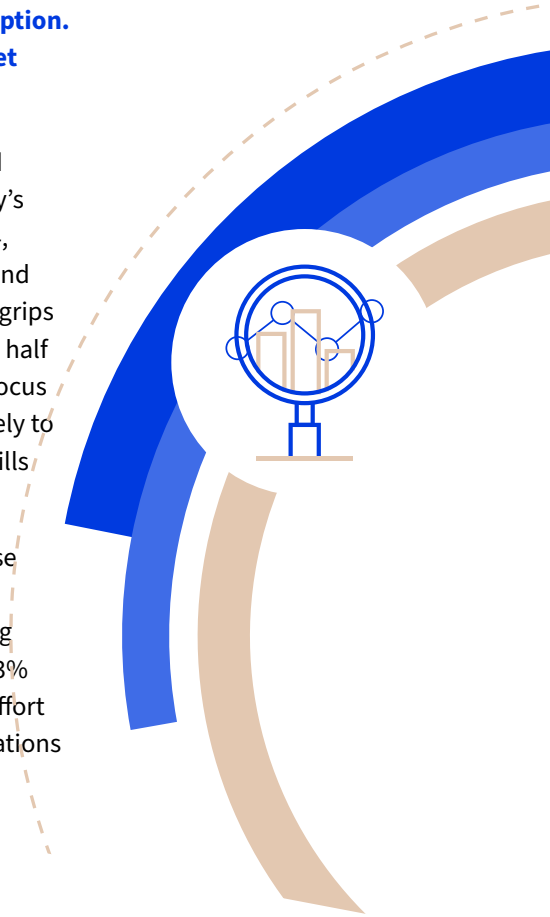
As organisations rush to adopt new technologies to gain competitive advantage in a volatile and fast-moving risk landscape, an iron-clad focus on strategy, risk management and skills will be key to success.

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.

AI promises to drag Europe's ailing productivity growth out of the doldrums, open new markets and boost profitability and competitiveness. But the challenges are steep. Few organisations have mature AI strategies backed up by solid governance processes – fewer still have a realistic roadmap for securing the talent needed to achieve that transformation. And with the increased cyber, data and reputation risk associated with AI, organisations have a delicate path to travel, balancing opportunity and threat at speed.

Risk in Focus 2025 draws on a survey of 985 CAEs, 5 roundtable events with 48 participants and 11 one-to-one interviews to map the key challenges, organisational responses and internal audit's remit over five hot topics:

- **Digital disruption, new technology and artificial intelligence (AI)** was the survey's fastest riser – going from 6th place in 2024, 4th place in 2025 and expected to rise to 2nd position by 2028. As organisations get to grips with strategy, regulation and people risk, half of CAEs expected it to be a top 5 area of focus for their functions by 2028, but that is likely to require a step change in internal audit skills and strategies.
- Deep fake attacks and increasingly intense AI-powered hacks helped **cybersecurity and data security** retain its long-standing position as the region's top threat with 83% saying it was a top 5 risk. Internal audit effort is well-matched in this area with organisations focusing on cyber defences and regulatory compliance.



Contents

- 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. Only 28% of CAEs ranked it as a top 5 area of internal audit effort suggesting a misalignment with the risk level for a significant number of businesses.
- **Macroeconomic and geopolitical uncertainty** dropped from its joint 3rd place ranking last year 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. By then, 40% of CAEs said it would be a top five area of effort – up from only 20% today. Upskilling internal audit functions is essential to meet that expectation.

With no sign of a let up in the velocity of risks in a wide range of interconnected areas across Europe, it is more crucial than ever for CAEs to support their organisations at a strategic level. While there is still disconnection between risk management and decision-making at the top of many organisations, the qualitative research found CAEs supporting boards to help bridge that gap.

These efforts have entailed pursing two inter-related strategies: to ensure the board is well-informed on how risks impact strategy, and to help drive better strategic decision making through scenario planning, for example, so that strategy is realistic, focused and able to flex. Such agility enables fast and proactive action on both risks and opportunities.

Less formally, directors are calling on CAEs to brainstorm on risk and strategy – and for them to provide support to decision-making processes. As one non-executive director said, "I encourage my CAEs to be bold and brave and be prepared to be involved in the decision-making process by, for example, challenging the assumptions of our decision-making processes."

Governance was the 2nd highest area of effort for CAEs with 64% saying it was a top 5 topic. While CAEs have consistently focused high levels of effort on governance processes in the Risk in Focus survey, this year many said it was also becoming a key tool for managing strategic risks.

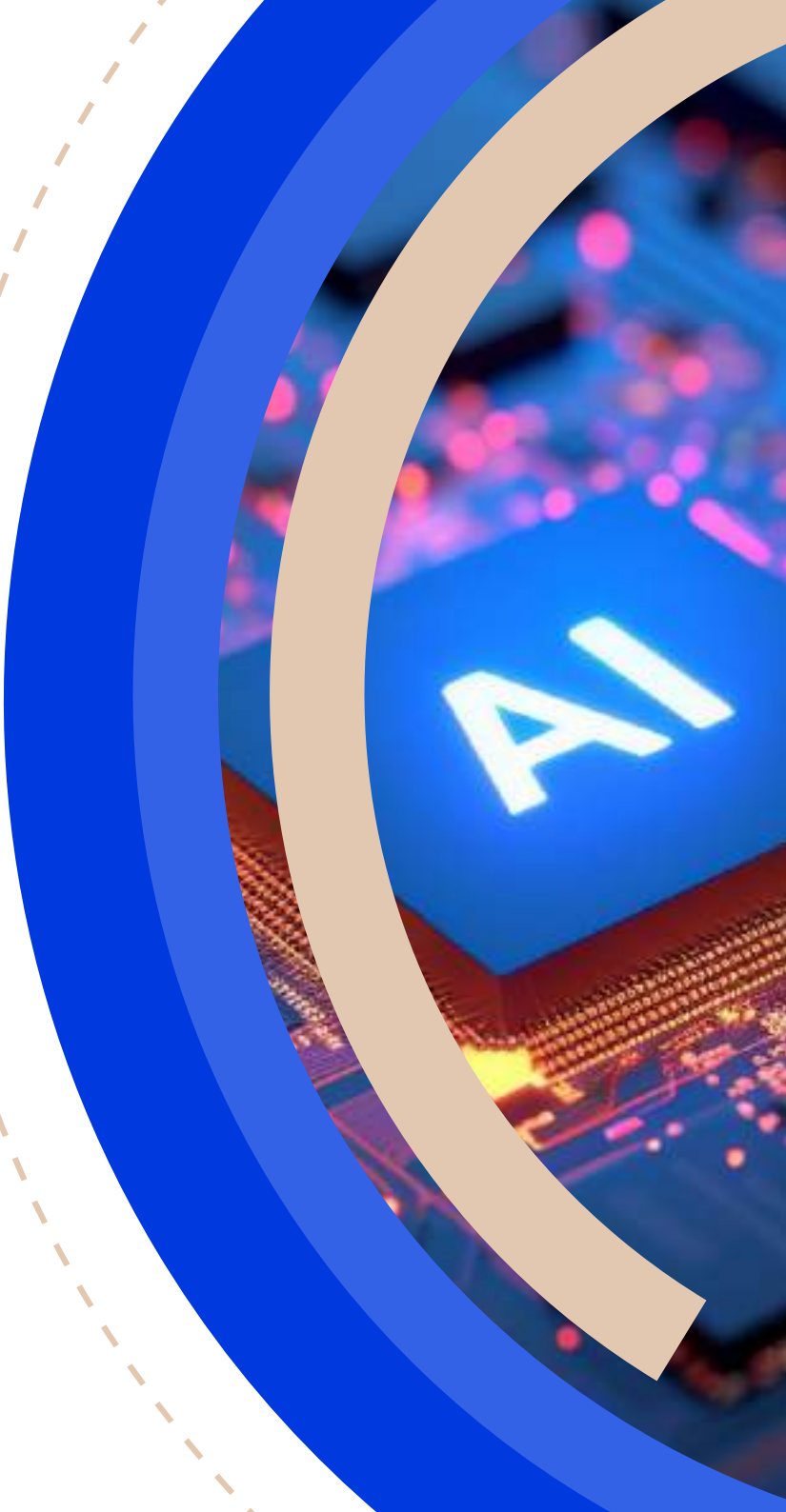
"With no sign of a let up in the velocity of risks in a wide range of interconnected areas across Europe, it is more crucial than ever for CAEs to support their organisations at a strategic level"

Contents

For example, in several roundtable discussions, CAEs said that they were increasingly using new regulatory requirements to improve governance processes and drive change.

But in some key areas – human capital, geopolitical uncertainty and climate change, for instance – internal audit effort falls short of the perceived level of risk. The reasons for those misalignments are discussed in the relevant sections of this report, but it is clear that more resources, training to upskill and reskill, and determination are needed if CAEs are to provide risk-based assurance on key threats.

That will be particularly so for digital disruption. Most internal audit functions incorporate digital auditing methods into their workflow, but few would describe themselves as being cutting edge. Securing talent in the two core digital risk areas – cybersecurity and new technologies such as AI – can be prohibitively expensive and (in a buyer's market) retaining those skills is tough. Acquiring and nurturing the right talent is more critical than ever when strategic digital initiatives depend on it. If CAEs are to hit their predicted levels of engagement in these areas by 2028, a step change in effort will be needed, including, perhaps, approaches that utilise integrated assurance strategies.



Contents

METHODOLOGY

In the first half of 2024, a quantitative survey was distributed among chief audit executives (CAEs) by 19 European Institutes of Internal Auditors, spanning 20 countries including Albania, Armenia, Austria, Belgium, Bulgaria, France, Germany, Greece, Hungary, Ireland, Italy, Luxembourg, The Netherlands, Norway, Poland, Portugal, Spain, Sweden, Switzerland and the UK. The project was conducted in partnership with the European Confederation of Institutes of Internal Auditing. This survey elicited a record-breaking 985 completed responses.

This year, 11 in-depth interviews were conducted with a range of CAEs, Audit Committee Chairs, Non-Executive Directors, academics and industry experts from various countries to identify the most pressing issues organisations face and key areas of internal audit focus. The results of this research informed the discussion topics for five roundtable events hosted with 48 participants in total, comprising mostly of CAEs but also including Audit Committee Chairs, Non-Executive Directors, academics and industry experts.

The analysis in this report was determined by the quantitative survey results, guided by the one-to-one interviews and enriched by the roundtable events. All participants contributed on the condition of anonymity. The format of this report builds on the success of a change in approach since Risk in Focus 2023 to take a deeper look into areas of pressing importance to internal audit and its stakeholders, rather than to only focus on the 5 top-rated risks each year.

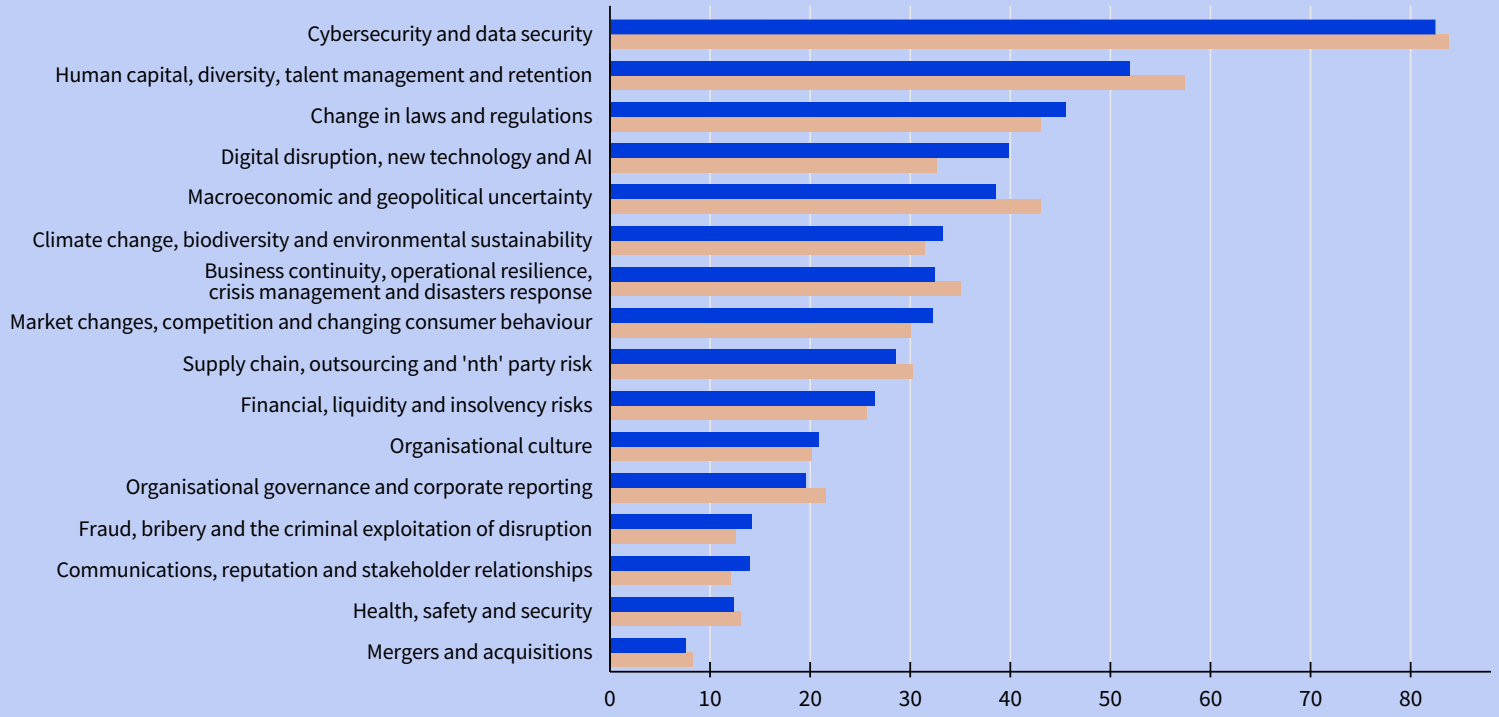
This report should not be considered prescriptive, but as a tool to inform internal audit's thinking in developing their internal audit plans and to provide a benchmark against which CAEs can contrast and compare their own independent risk assessments.

We hope that CAEs will use this report as an agenda item for audit committee discussions and as a tool to support their internal audit planning and strategy. The report is also of relevance to a broader range of governance stakeholders including audit committee chairs, board members, risk management, along with other assurance and governance professionals.

A Board briefing is also available so that CAEs can engage stakeholders in conversation about key survey findings. In addition, there will be a series of follow-on roundtables.

What are the top five risks your organisation currently faces?

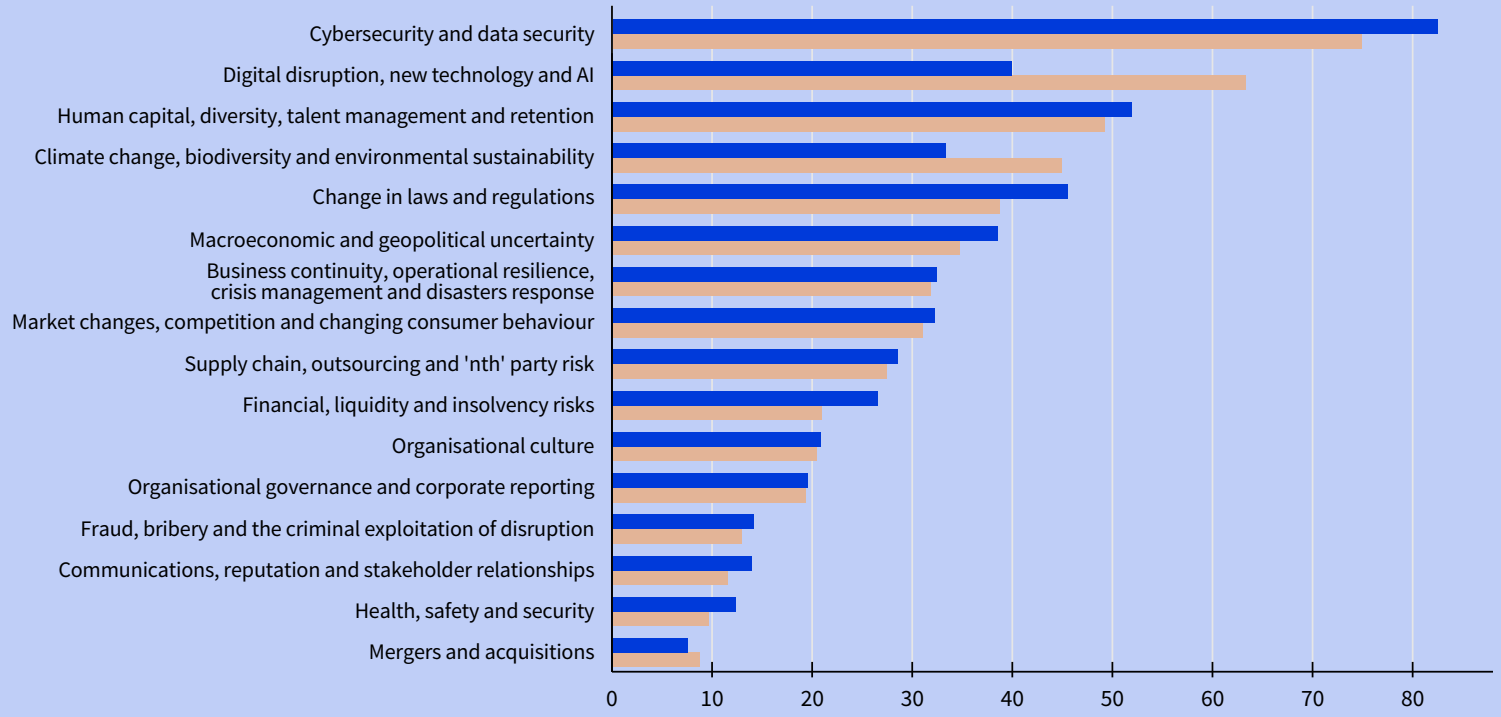
Digital disruption, new technologies and AI was the fastest rising category. Organisations are under intense pressure to ramp up efforts to meet growing market demands and keep up with competitors.



Looking ahead

What do you think the top five risks to your organisation will be in three years' time?

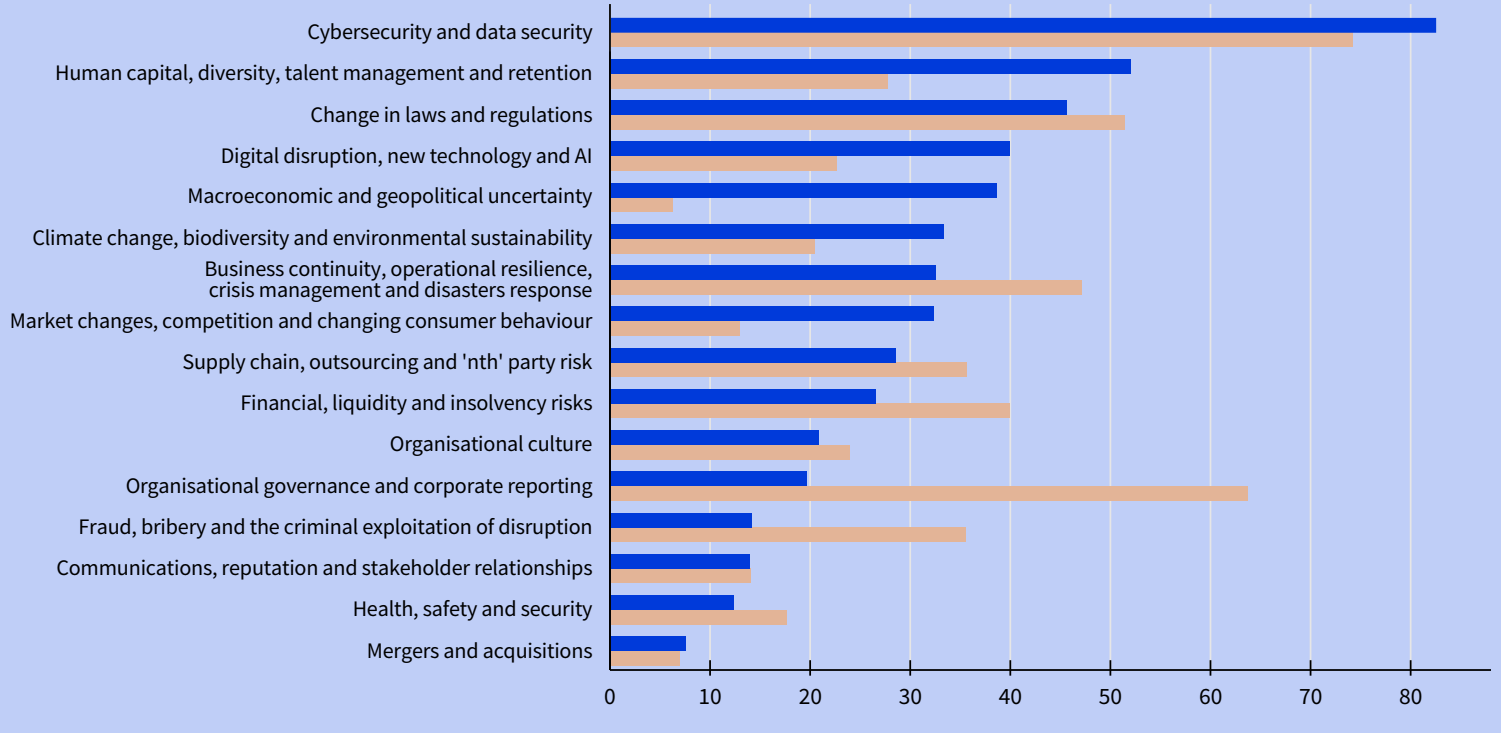
Technology risks will dominate the rankings by 2028 with climate change risk becoming a top 5 risk. The persistence of people risk suggests organisations may struggle to attract, develop and retain the right talent to meet these challenges.



Risk priorities vs. audit's focus

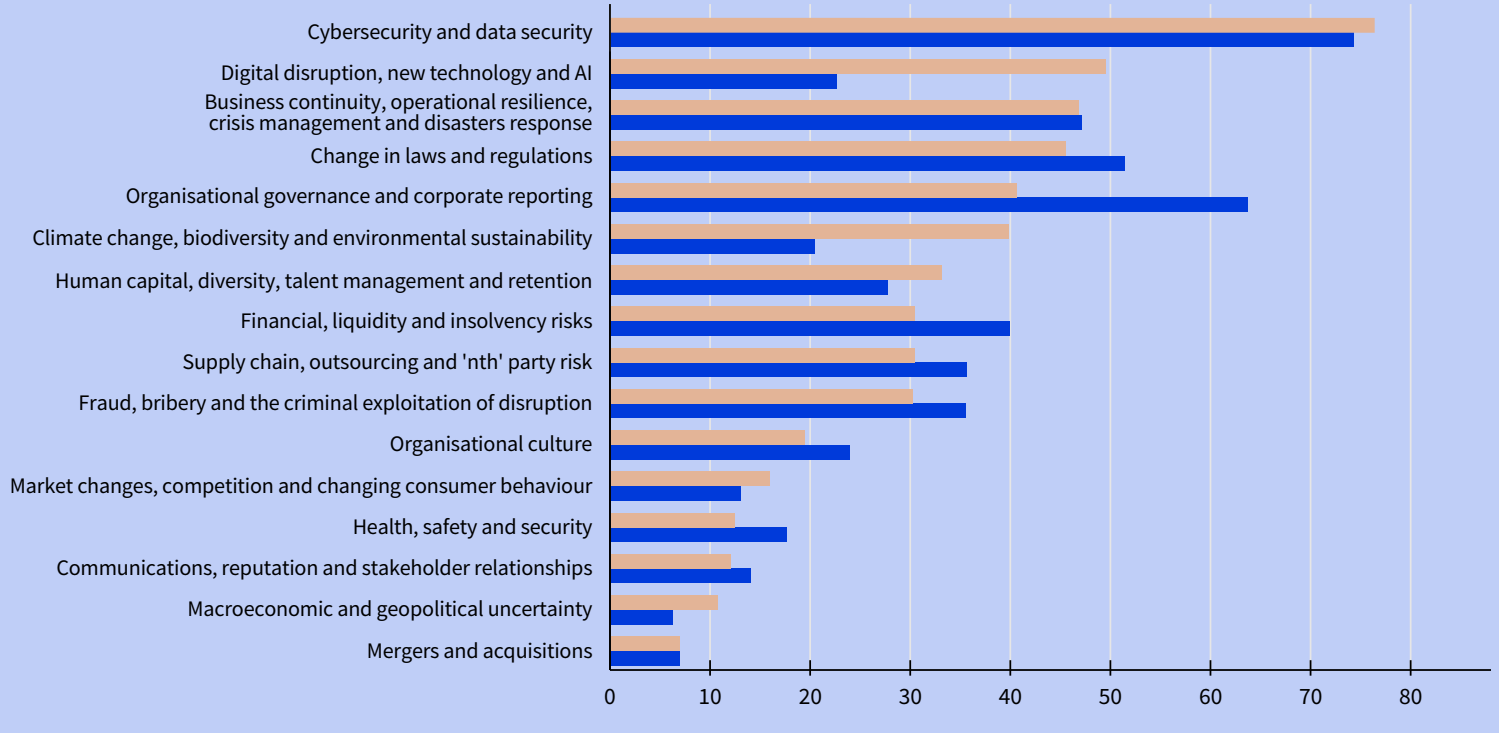
Top 5 risks compared with where internal audit spends the most time and effort

Internal audit effort is misaligned with human capital, digital disruption, new technologies and AI and macroeconomic uncertainty with time spent increasing slowly due to issues such as skills shortages, lack of knowledge and risk categorisation. CAEs were aligned better in traditional areas such as organisational governance, corporate reporting and cybersecurity.



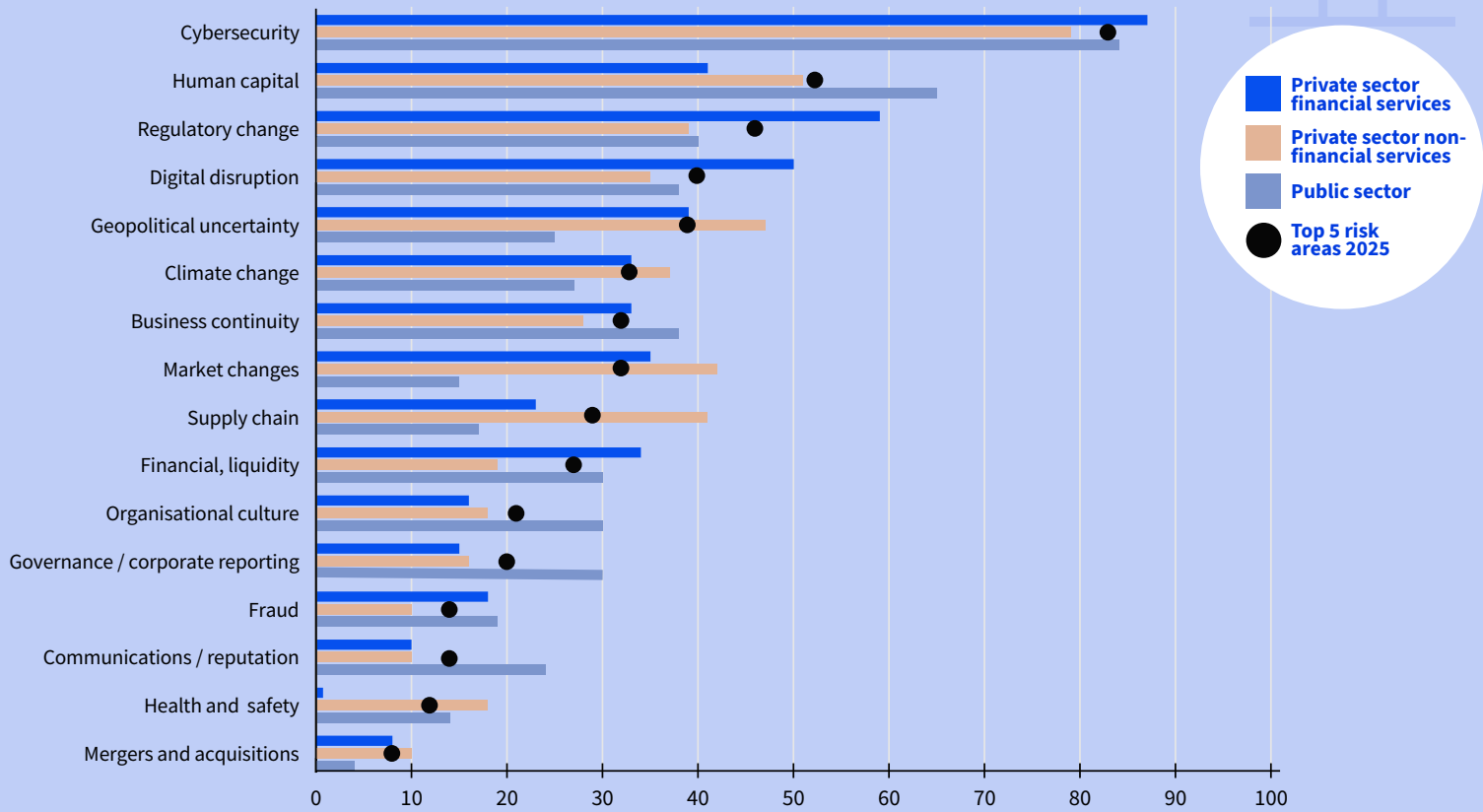
What are the top 5 risks you expect internal audit to spend the most time and effort addressing three years from now

While internal audit alignment with key risks looks better balanced by 2028, attention on the fast-rising risks – digital disruption and climate change - will lag, raising the possibility that some functions may struggle to keep up with their organisations' needs.



Top 5 risks by sector

All sectors rank cybersecurity as the highest risk. For financial services firms, regulatory change and digital disruption also present significant challenges, whereas non-financial private enterprises rated geopolitical uncertainty and market changes highly. Human capital risk was higher rated among public bodies compared with other sectors.

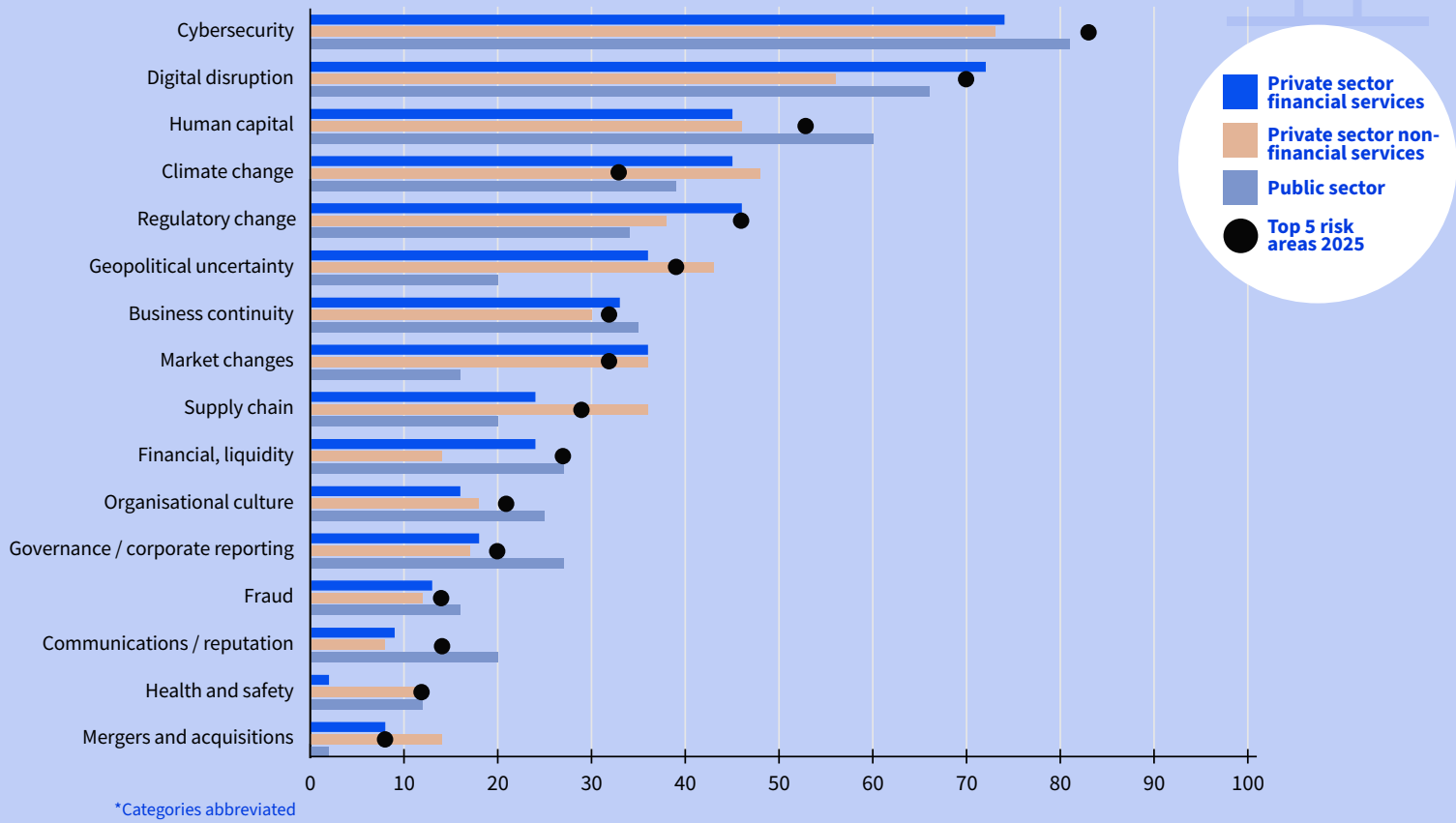


*Categories abbreviated

Key survey findings

Top 5 risks in three years' time

Cybersecurity again tops the risk ranking in 2028. Digital disruption, new technologies and AI rise to second place overall in the risk rankings, with it being particularly challenging in the private sector financial services realm.



*Categories abbreviated

DIGITAL DISRUPTION, NEW TECHNOLOGIES AND AI

Renewing digital disruption strategies

Publicity around artificial intelligence has accelerated organisations' attempts to gain a strategic advantage through their digital transformation projects

The advent of generative artificial intelligence[1] (gen AI) has given fresh impetus to organisations' digitalisation efforts, helping to boost the strategic importance of new technologies. For example, while half of global organisations reported adopting AI in at least one business function over the past 5 years, that figure has risen sharply to 72% in 2024 with many saying they have adopted it in multiple areas, according to McKinsey. In other words, interest in gen AI has fuelled an intense focus on retooling all AI and digital processes within businesses.

Digital disruption, new technology and artificial intelligence was the fastest growing risk area in this year's survey – and represents a predominant theme in this year's report. CAEs expected it to rise from the 4th most pressing threat this year to second place by 2028. And with 49% of CAEs saying it would become a top 5 area of internal audit assurance focus by 2028, it will move to 2nd place on that metric. That would require a rapid upskilling for some internal audit teams suggesting that human capital effort in this area has become strategically important (see also human capital, diversity, talent management and retention, page 22).

He said both businesses and politicians tend to be too short-sighted in their responses to rapid technological innovation that is happening outside the region "When organisations face these dramatic economic and competitive risks, CAEs are in danger of overrating the local threats their own companies face and hugely underrating the risks arising from outside of Europe that will hit them".

Strategic risks

While organisations have seen digitalisation as a disruptive force for many years, AI represents a revolution within that revolution. The speed of its development has been rapid recently, especially since gen AI became a public sensation in 2022 with the launch of the consumer-friendly ChatGPT. Its popularity and the rapid integration of AI into services offered by major technology companies has helped make the safe adoption of all AI a key issue for boards.

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

[1] Generative artificial intelligence is a machine-learning model that creates new data based on data contained in its learning set, "Explained: Generative AI," MIT news.

DIGITAL DISRUPTION, NEW TECHNOLOGIES AND AI

"If organisations do not have AI in their strategy, they will not be successful in the future," said a CAE at a major German technology company in an interview for this report. He said that AI would accelerate competition risk as organisations needed to both implement efficiencies to manage costs and to be able to rapidly innovate new products and services to meet shifting market expectations – underlining the persistence of market and competition in 7th place in this survey. Businesses' future digitalisation and AI strategies must be underpinned with an effective change-management plan and an AI-specific human resources strategy, he said.

Unfortunately, CAEs at the roundtable said digitalisation was often piecemeal and divorced from the strategic objectives of their organisations. Since gen AI, for example, is freely available and cheap, projects can spring up randomly and it can be difficult to map AI use in the business – which also creates a cybersecurity and data risk.

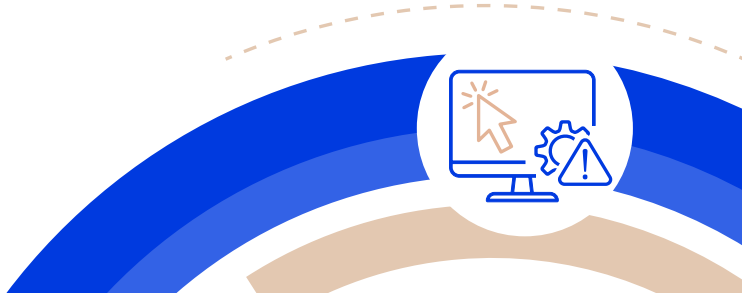
To combat fragmentation, many businesses are striving to centralise, control and direct those efforts. For example, a CAE at a French aircraft manufacturer said her company had created a centre of AI excellence to ensure all such projects across the organisation were managed centrally and aligned with strategy. While effective, demand from the business currently outstripped its capacity, she said. CAEs said they were reviewing their organisations' strategic risk registers to map where AI was deployed and to create a complete overview of the state innovation across the enterprise.

In addition, CAEs said that their organisations had started supporting the development of AI governance policies and guidelines, but some admitted that it has been difficult to operationalise included principles effectively. "Artificial intelligence is transversal because it can affect many parts of an organisation," said a CAE at a Spanish energy company. "We have specialist IT teams that are not centralised and, although they have good governance around their processes, that does not map onto the more holistic overview that we need for AI."

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

Regulatory patchwork

The European Union's Artificial Intelligence Act (AI Act) is the world's most prominent regulatory framework for AI globally. The UK government's principles-based, non-statutory framework is less prescriptive than the AI Act. But because international regulation is developing rapidly it could create a patchwork of conflicting requirements for global businesses – helping to keep compliance with regulations at 3rd place in the risk rankings.[2]



[2] The USA alone has 650 proposed state bills that relate to AI in 2024, according to Computerworld.

DIGITAL DISRUPTION, NEW TECHNOLOGIES AND AI

CAEs taking part in the report's qualitative research said that the AI Act had helped them raise awareness in the board of the potential risks. But during the roundtable, many agreed that the guidance it contained was still incomplete and therefore of limited use in helping organisations to create, for example, an AI governance framework. A key problem is the risk-based approach that EU regulators have taken. It defines four levels of risk for AI systems: unacceptable, high, limited and minimal. Yet CAEs said that they were unable to clearly understand the borderline between the middle two categories because the guidance is not detailed enough.

"Currently, there are no concrete governance frameworks we can apply," according to a German professor of internal auditing at the roundtable. He said that AI guidance by, for example, OECD tended to be too broad, while other regulation such as NIS 2's updated cybersecurity framework was too narrow. "CAEs are actually stuck in the middle between super-general approaches and really detailed approaches," he said.

This lack of clarity could mean that AI-enabled products rushed to market risk being either non-compliant or will reach consumers too late if organisations wait for clarity.

With so many CAEs focusing on governance frameworks, and audit methodologies specifically designed to assess AI, most said they were planning to provide assurance over small, specific use cases as well as AI governance processes over the coming 12 months. In addition, some CAEs in technologically developed businesses are integrating AI in their internal audit processes in areas such as controls monitoring.[3] Most others said they were still working on improving their general audit automation programs as a priority.

People risk

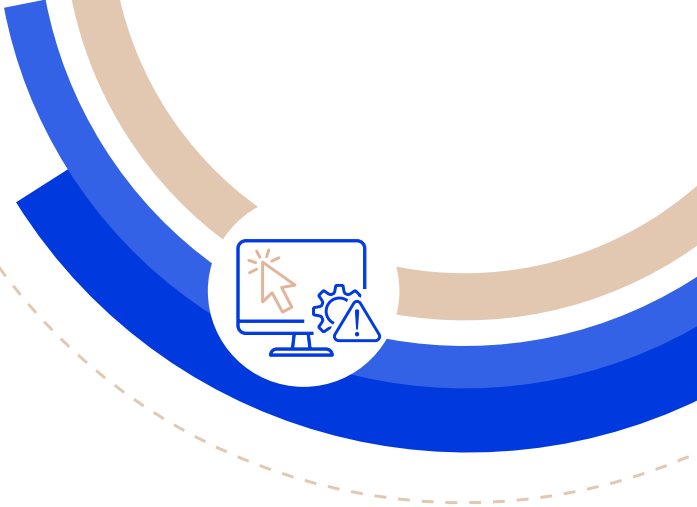
AI-specific skills are hard to find at all levels – including the board – and for CAEs skilled staff and technicians are often too expensive. With resources tight, CAEs are looking to partner with those in the first and second lines to help with skills deficits.

Yet CAEs can play a key role in supporting recruitment efforts across the business. "Internal audit can help the business by auditing how human resources is dealing with artificial intelligence skills risk in particular," a CAE at a Spanish infrastructure group said during an interview for this project. Recruitment policies and practices had to be tightly aligned with AI strategy for the business to acquire and develop the right skills and to help smoothly integrate software into the business, he said.

"Internal audit can help the business by auditing how human resources is dealing with artificial intelligence skills risk in particular"

[3] See ECIIA's 2023 position paper, Auditing a Digital Insurance World - Artificial Intelligence and Machine Learning audits within Insurance Firms.

DIGITAL DISRUPTION, NEW TECHNOLOGIES AND AI



Ethical and operational risks

Organisations are also seeking to deal with the complex ethical risks associated with the use of AI by banning its use in applications that have an external interface. Some CAEs at the roundtable event said their businesses had completely prevented the use of gen AI because of a range of known faults inherent in such programs: the unintended publication of confidential company data, the existence of bias and prejudice, and the lack of transparency and fundamental inaccuracy in some AI output. With so many interconnected risks, one CAE said he was planning to assess each new AI initiative from multiple perspectives. “Each audit assignment will take into consideration privacy, data governance, transparency, diversity, social risk and environmental exposure,” he said.

But fundamental problems could remain. If inaccurate data processed by AI leaks into strategic decision-making processes, that could prove costly. CAEs agreed that trust could, therefore, remain a major issue for AI systems, especially with the rise of AI powered deepfake cyberattacks and disinformation (see cyber security and data security, page 17). They advocated for an increased focus on critical thinking both throughout their organisations and within internal audit functions. That is in line with the revised Global Internal Audit Standards 2024™, which added professional scepticism as Standard 4.3.

How internal auditors can help organisations

1. Assess how well the organisation’s AI and digitalisation strategy is supported by a credible business transformation or change-management plan
2. Provide assurance that individual AI projects are linked to the main strategic objectives of the organisation
3. Provide assurance that the organisation’s governance processes are able to control the strategic and effective deployment of AI across the business
4. Assess how well processes are compliant with current regulations, such as the AI Act, in the relevant jurisdictions and include regular monitoring and intelligence gathering
5. Provide assurance that the organisation’s AI strategy is underpinned by a skills and talent programme that can attract, develop and retain key capabilities
6. Provide assurance that the organisation’s use of AI in particular is ethically sound and is seen as trustworthy in the marketplace

CYBERSECURITY AND DATA SECURITY

Tackling hybrid cyberattacks

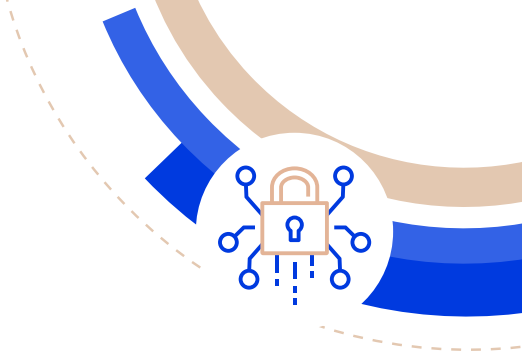
Hackers are exploiting AI to increase the number, velocity and sophistication of attacks in ways that blur traditional risk categories.

Cybersecurity and data security retained its position as the most pressing risk for organisations in 2025, suggesting getting ahead of the fast-moving threat landscape remained elusive. Eighty-three percent of respondents said it was a top 5 risk – almost 4 in 10 (37%) said it was their top priority. Internal audit effort is well aligned with 74% of respondents ranking it as a top 5 area of effort.

83% of respondents said **cybersecurity and data security** was a top five risk. Almost 4 in 10 (37%) said it was their top priority.

Threat landscape

The velocity and volume of cyberattacks climbed sharply over the past few years. Phishing attacks in the US alone increased by 1,265% in 2023 thanks partly to the growth of generative AI (gen AI), according to one report. It is a trend that has intensified every year since Risk in Focus 2017. Pressure on organisations to detect and respond to potential attacks rapidly is intense – many CAEs at the roundtable said that they had increased their own AI-powered controls monitoring as a result. In addition, Europe is now engaged in a covert cyberwar with state actors targeting critical infrastructure, financial systems and operational networks – including third party suppliers (see macroeconomic and geopolitical uncertainty, page 27).



CYBERSECURITY AND DATA SECURITY

New AI-powered techniques are blurring traditional risk categories where businesses have generally considered external and internal threats to be related but separate issues. Recently, for example, AI-generated deepfake cyberattacks that impersonate key personal mean that external threats have appeared on what look like credible, internal systems. Both UK firm Arup and advertising multinational WPP were targeted in 2024 by such attacks.

"The more sophisticated the attack, the greater the concern," a UK non-executive director said in an interview for this project. "That is why people are becoming a more crucial part of our defences than ever." At many businesses, he said, employees faced mock attacks each week. Those exercises were reported to IT and linked to targeted training and coaching. Internal audit provided assurance over the process.

In some case, external actors are aiming to gain entry to businesses physically. A CAE at the roundtable said his organisation (a French consultancy) had seen a rise in what he called hybrid, or "phygital" attacks – cases where employees with fake IDs had attempted to gain employment in key areas of the business. "The physical processes have been reinforced to make sure there is no impersonation in the people we recruit," he said. "Human resources are now more closely tied into our broader security defence procedures."

Yet internal IT weaknesses are still targeted via external penetration. In 2024, it took an average of an hour for hackers to move laterally across a business once they penetrated defences – down from 84 minutes a year ago. Without strong and clear governance processes around existing and new technology implementations, the impact of an incursion could be severe. And while user authorisation and access management has always been an important field of activity for internal audit, CAEs said they are urging organisations to treat it as a business rather than an IT issue.[4]

A Swiss assurance consultant said his firm spent about 60% of its time in 2024 providing identity and access management audits to clients. "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," he said. A CAE at a German tourism business said that he communicated the results of IT security audits to the CIO, management and the board and ensured there were opportunities to discuss their significance.

"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"

[4] For more on internal audit's role, see Global IIA's 2022 GTAG guidance Auditing cybersecurity operations.

CYBERSECURITY AND DATA SECURITY

In fact, when asked which risks would be most negatively impacted by AI, CAEs identified cybersecurity and fraud as the top two threats, followed by digital disruption and human capital. On the other hand, increased digitalisation also promises to strengthen defences. As well as working to develop cultural awareness related to such risks, many businesses are strengthening data analytics and AI-empowered defences (through, for example, pixel analysis techniques) in response.

"We have moved more to a consulting approach with new technologies so that controls are set up properly and to ensure alignment across the three lines in strategic IT implementations," a CAE at a major European financial exchange said in an interview for the report. In 2024, there was a major focus for her team to ensure the first and second lines were operating the right controls and assessing the design and operational efficiency of those processes. "The key for internal audit is that it can see the whole value chain, identify gaps and weaknesses where they exist and strengthen our defences," she said.

Regulatory compliance

This year, CAEs are helping their organisations get ready for two core pieces of legislation aimed at harmonising regulation and improving digital resilience across Europe – the Digital Operational Resilience Act (DORA) and the NIS 2 Directive.

DORA affects financial firms (and finance-related subsidiaries) – approximately 38% of survey respondents worked in this area.[5] The regulation provides internal audit with a legally defined role, but most affected CAEs attending the roundtable said that risk assessments, security and data controls were already established. The exercise was "more like fitting existing parts into DORA's categories," said one.

[5] See ECIIA's 2023 paper The digital operations resilience act and its impact on internal auditors in financial services

CYBERSECURITY AND DATA SECURITY

While the audit universe had not changed greatly, those risk areas were now becoming overlaid with an additional compliance risk, a CAE at a German tourism business said.

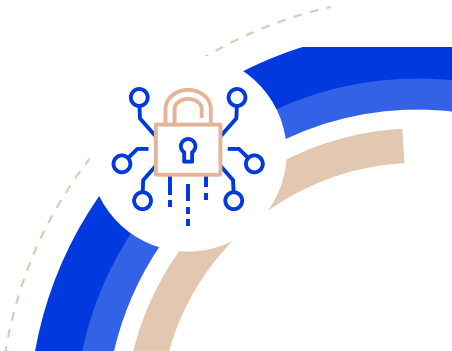
NIS 2 affects large and medium-sized enterprises across the EU in 18 sectors.[6] The deadline for Europe's member states to transpose the requirements of NIS2 into national law is 17 October 2024, meaning compliance dates will be staggered across the zone – and UK businesses have been put on notice that similar changes are afoot.

Most CAEs said they were already auditing their organisations' readiness for NIS2. Sometimes that work had been intensive. One French business consultancy had, for example, integrated NIS2's six chapters into its governance framework – including within group internal audit. That would enable internal audit to provide assurance on cyber and data security governance across all entities, said its CAE. A CAE at a German car manufacturer said his first audit on NIS2 readiness took place in 2022 on ransomware processes. That had exposed some weaknesses in, for example, their ability to respond to such events – including its risk appetite for paying over money – and had strengthened the end-to-end response processes.

Two big lessons have been on connecting risks and on the effectiveness of monitoring. "First, there is a tendency to have an IT tool to separately document, score and monitor processes with legal requirements underpinning those," he said. "But you do not develop a holistic picture if you are only checking elements individually and you are likely to miss the bigger picture," he added. Second, effective monitoring is critical. That is why on cybersecurity, in particular, the business is developing a dashboard to boost its monitoring capabilities based on internal audit's recommendations.

In 2024, the German car manufacturer's CAE focused audits on third-party cyber-risk management, especially in relation to IT systems integration because of potential cyber-vulnerabilities in some partners. Third party suppliers, including cloud services, were a major concern for roundtable attendees. CAEs are using the requirements set out by DORA and NIS2 to pressurise reluctant suppliers to be open about their risk assessment processes – and to require audit access where extra assurance is needed. A CAE said that one third-party audit had revealed that documented controls were completely absent in reality. Boards have supported such strategies given new corporate liabilities for poor controls under NIS2. It is a trend identified by this research that CAEs are increasingly using new laws and regulations as an opportunity to improve their organisations' resilience.

CAEs at the roundtable said they saw potential for internal audit to use AI to help the business in a range of areas, including providing assurance that AI outcomes and company policies are aligned with ethical outcomes and in automating cyber defences.



[6] A medium-sized organisation is defined as having 50 or more employees, or an annual turnover and balance sheet total of €10 million or more, but other factors may apply.

CYBERSECURITY AND DATA SECURITY

How internal auditors can help organisations

1. Provide assurance on the security culture around cyber-risk and whether training is regular, relevant and the results of testing well communicated
2. Provide assurance that departments are fully updated and aware of potential hybrid attack methodologies for the impersonation of employees and that controls are robust and tested
3. Assess how well the organisation escalates cybersecurity, and identity and access management findings and whether these are adequately discussed at all levels of the business
4. Provide assurance on the governance systems and processes including whether the three lines work effectively together
5. Provide assurance that NIS2 framework (and DORA where relevant) is integrated into the organisation's governance framework and on regulatory implementation and compliance
6. Provide assurance that controls monitoring is approached holistically to avoid blind spots and that results have high visibility

HUMAN CAPTIAL, DIVERSITY, TALENT MANAGEMENT AND RETENTION

Aligning human capital and business strategy

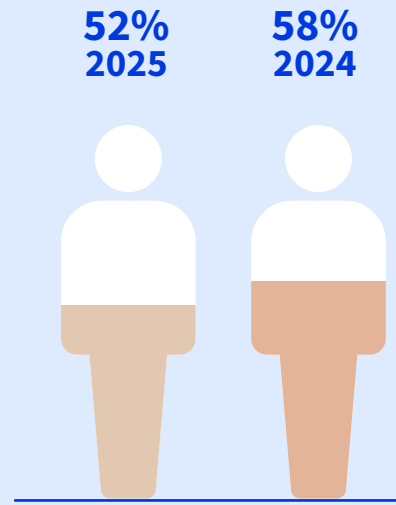
Organisations are working towards better alignment with their employees' changing requirements but retooling HR strategies for a more digital future remains a challenge.

Human capital issues retained their position as the 2nd biggest threat identified by the survey with 52% of CAEs saying they were a top 5 risk for 2025. By 2028 it will rank 3rd just behind digital disruption, new technology and AI, but ahead of climate change.

With a renewed focus on boosting digital skills in the survey this year, human capital is a key strategic and competitive risk for organisations in all sectors. Yet only 28% of CAEs said it was a top 5 area of internal audit effort for 2025 – a figure that is expected to climb to only 33% by 2028 despite its persistently high ranking as a top 5 risk for organisations.

Not all CAEs that identify talent management as a top 5 risk are able to provide adequate assurance and advisory services in that area. For example, one CAE at the roundtable said that their human resources department declined an offer for internal audit to help; others said they often lacked the skills and resources to work effectively in this field. Whether other assurance providers in the business are engaged in this strategically important area is a topic of possible future research – but the mismatch of assurance focus and risk over the past few years of Risk in Focus should serve as a red flag for CAEs.

Several IIA Institutes are working to provide tools and guidance for auditing behavioural risk, risk culture and organisational culture – and to assess how those areas align with strategy and business values. A member of the Chartered IIA in the UK at the roundtable said that discussions relating to the revised Code of Practice focused on 3 key areas.



52% citing **human capital, diversity, talent management and retention** as a top five risk this year compared to 58% last year.

HUMAN CAPITAL, DIVERSITY, TALENT MANAGEMENT AND RETENTION

One, internal auditors would collaborate with behavioural scientists to learn how to use the latest scientific models in their audit work. Two, internal audit functions would use that knowledge to challenge the design of HR processes in routine engagements including, for example, recruitment, remuneration and retention. Three, internal auditors would assess the alignment of behavioural risk management to strategic initiatives. Such tools may improve CAE's effectiveness in this area.

Demographic and social challenges

In the wake of the COVID-19 pandemic, harnessing the power of a multigenerational workforce remains a major challenge among shifting expectations of work. CAEs at this year's roundtable said that workers in all age groups were seeking a better work-life balance, access to learning and development, a greater focus on employee well-being and for the companies in which they worked to demonstrate strong social values.

To assess changing attitudes and needs, many organisations rely on employee surveys, which can be insightful although results and recommendations often remain unimplemented. To deal with such issues, a CAE at an Austrian bank, for example, said that while internal audit had measured the culture of the group through an assurance audit, the business also created small working groups to deal with the specific issues from the audit. The action plans from those were collated and presented to the leadership council, itself overseen by the chair of the board.

A CAE working in the financial services sector in Albania said the rate of staff turnover was increasing annually. While that may lead to a drop in institutional knowledge, there is also a risk that some long-serving staff fail to adapt to the changing needs of the business.

HUMAN CAPITAL, DIVERSITY, TALENT MANAGEMENT AND RETENTION

"Whenever we conduct an audit, we check to see if we have a healthy rate of attrition," the CAE of a French IT services business said. "If it is too low or too high, we look into the root causes."

Sometimes internal recruitment processes can be too difficult for staff to navigate, leading to businesses losing talent unnecessarily. The French CAE said that his internal audit function was reviewing recruitment processes across the business to help break down any institutional silos restricting the movement of talent across the group.[7]

Improving the efficiency of human resources processes is vital. "It is likely that people will cycle through organisations more often than they used to because they are looking for different things," a consultant at a leading UK consultancy said in an interview for this project.

"Organisations need better onboarding processes to get people up and running much more quickly – and better exit processes and exit interview management so that you can really understand why people are moving on."

Developing clear and transparent messaging both inside and outside the business on its values, policies and ambitions for its employees could reap benefits. A CAE at a financial service group in the Netherlands said that the European Union's Corporate Sustainability Reporting Directive (CSRD) required companies to disclose their human resources strategies and policies in the report, including on work-life balance, diversity and wellness, and that document would need to be verified by an external assessment. "CAEs can align their internal audits with these metrics to help provide assurance to the business that its strategic objectives are on track," he said. It is one of several areas identified in this report – along with cybersecurity and climate change – where CAEs are leveraging the compliance requirements of regulation to help improve effectiveness and resilience.

"Organisations need better onboarding processes to get people up and running much more quickly – and better exit processes and exit interview management so that you can really understand why people are moving on"

HR departments play a key role in creating a culture that is both welcoming to staff and relevant to their organisations' strategic objectives. But one survey suggested that while many HR departments rated their performance high in providing good employee experience (64%), only 20% of employees agreed. Another survey said that European employees had the highest level of disengagement globally.

[7] Note that Global Internal Audit Standards 2024™ now require a specific and dedicated approach for developing the retaining internal auditors.

HUMAN CAPITAL, DIVERSITY, TALENT MANAGEMENT AND RETENTION

As well as increasing attrition and turnover, "there is a danger that such disengagement turns into some form of fraud or unwanted behaviour," the director of a UK internal audit training consultancy said at the roundtable.[8] Useful tools are available for management to get to grips with such disconnection by, for example, focusing on those elements of psychological safety that help promote committed and high-performing teams. Internal audit functions could assess whether such initiatives are in place and are effective.[9]

Digitalising HR

Digitalising HR processes can bring benefits. For example, implementing an enterprise-wide human resources system can provide the business with the data it needs on recruitment, retention and attrition. Digitalisation can also help the HR function build a user-interface on its digital and mobile services so that interaction with the business has the same look and feel as everyday apps that are popular to improve engagement.

Yet while CAEs at the roundtable were supportive of such initiatives, they expressed caution over the use of artificial intelligence (AI) in HR processes because of known problems of bias – and wider concerns of trust. "At the beginning of this process, internal auditors need to look at the governance of AI in these areas and, of course, the ethics associated with AI use," said the CAE from the Austrian bank. It will also be necessary to consider the categorisation levels in the European Union's AI Act to make sure any processes are compliant with that legislation.

Strategic workforce planning

Given that most organisations are struggling to attract and retain the skills and talent to implement digital transformation initiatives at the same time as adapting to rapidly changing workforce trends, longer-term strategic workforce planning has become extremely complex. HR departments are often not front-runners when adopting AI into their processes – the top barrier being lack of integration into enterprise IT systems.

[8] See ECIIA 2022 paper Risk overview, human capital, diversity and talent management for strategies.
[9] See IIA Netherlands 2024 paper on Psychological safety, tools for Internal Audit.

HUMAN CAPITAL, DIVERSITY, TALENT MANAGEMENT AND RETENTION

CAEs said having the right leadership and tone from the top, focusing on excellent change management, upskilling in key areas and creating a HR strategy fitted to a longer-term change programme, were all seen as critical.

Strategically, CAEs have a key role to play in clarifying to the board the interdependencies between succession planning, inclusion and diversity, ESG and culture to help it in strategic decision making. “Areas such as strategic workforce planning have become so complex that whatever plan we come up with will almost certainly be wrong,” the UK consultant said in her interview for this project.

> “But there must be a clear direction of travel around which the organisation can flex and it is internal audit’s role to make those issues clear to the board”

How internal auditors can help organisations

1. Provide assurance that workforce planning is effective in both recruitment and retention and is aligned with strategic objectives
2. Assess whether HR policies and procedures are aligned with the demands and social values across the organisation’s different social and demographic groups
3. Provide assurance that employee surveys are properly conducted, and that follow-up actions and plans are implemented effectively
4. Assess whether the organisation’s attrition rates are within healthy levels and help management understand the root cause of any problems
5. Provide assurance that organisational procedures aid the recognition, movement and promotion of key talent across the entire enterprise, as well as support swift onboarding and exit processes
6. Support the board in understanding the interdependencies between succession planning and diversity, equity and inclusion so that strategic decision making has a clear focus and purpose

MACROECONOMIC AND GEOPOLITICAL UNCERTAINTY

Seeking greater clarity

In an increasingly volatile geopolitical environment, organisations are integrating emerging risks into their strategic governance processes.

The inflationary price shocks peaked in Europe between 2022 and 2023 and then lessened in 2024, with interest rates hovering at above 2.5% at the time of writing. While that may have eased upward pressures on the cost of both doing business and living, the risk from possible market changes and competition remained the 8th most pressing risk for 2025. But the greater shock for business was the eruption of war in Palestine and the disruption of trade routes in the Middle East – along with the threat existing wars intensifying or new conflicts breaking out.

Not surprisingly, then, uncertainty surrounding the world economy and the political situation remained a top 5 risk for 39% of CAEs in this year's survey. Yet only 6% of CAEs said they spent significant internal audit time on the issue. CAEs at the roundtable said that regulated industries, such as the financial services sector, needed to report on such topics directly.

But other organisations tended to focus only the risks that flow from these events, including supply chain disruption, cybersecurity and financial resilience – and actions such as stress testing, scenario planning and business continuity programmes. That suggests internal audit engagement[10] is under-reported by the quantitative data.

But participants disagreed over whether, war and conflict, for example, should be a specific topic for risk registers so that organisations did not miss the bigger picture. "When you have a transverse risk, one that affects multiple things at once, it is a problem for standard organisations that are organised vertically to fully capture the complexity of possible impacts," said one CAE at the event. CAEs agreed that as a result, periodically reviewing risk categories across their organisations was essential.

[10] See also, Chartered IIA's Navigating geopolitical risk.

MACROECONOMIC AND GEOPOLITICAL UNCERTAINTY

War and conflict

Digitalisation and new technologies mean that conflict in the 21st century goes beyond direct combat between armies. For example, the reported rise of state-sponsored cyberattacks across Europe suggests an intensifying of hostilities by Russia and China, at the same time as new technologies have given smaller states greater power to disrupt global trade. This so-called "grey zone aggression" is exemplified by attacks on shipping in the Middle East. "Partly because the Houthis are a non-state actor, it is difficult for the West to find an effective deterrent response," a report by the consultancy wtw said.

Strategically, businesses are increasingly treating the topic as a governance issue. "In a volatile world, resilience has moved from historically being about having enough capital and strong cybersecurity, to how fit your business model is, and how robust your governance processes are" a UK audit committee chair working in the financial services sector said at the roundtable. Stress testing organisations' strategies and operations has become critical and CAEs should provide assurance that processes around the first and second line are robust and accurate, he said.

"In a volatile world, resilience has moved from historically being about having enough capital and strong cybersecurity, to how fit your business model is, and how robust your governance processes are"

"In the financial industry we have very strict rules on stress testing, which need to be accurate, relevant and timely," a CAE at a French financial services firm said. "That testing gives us the ability to be agile to deal with volatility and spot opportunities. Other industries would benefit from this approach."

CAEs at the roundtable cited additional impacts from conflict in health and safety, and the supply and development of core digital technologies such as computer chips and AI systems. Tactically, business and assurance efforts should be focused on boosting resilience for manufacturing key products, and unexpected increases in the cost of goods, services, and finance, they said.[11]

[11] See, Chartered IIA's 2023 Adapting to economic uncertainty: internal audit's journey.

MACROECONOMIC AND GEOPOLITICAL UNCERTAINTY

Regulations, trade embargoes and sanctions

Trade embargoes and sanctions have also become another area of grey zone aggression – helping keep changes to laws and regulations 3rd place in this year's survey. For example, in 2024 the Dutch chip manufacturer ASML was banned by the US from supplying Chinese businesses with products and services – a region that represents about half of the company's revenue geographically. In 2022, US sanctions against Russian banks prevented the Belgium-based international payments firm Swift from dealing with them.

While such moves have a profound and immediate impact on those affected, CAEs at the roundtable said second and third order impacts could be difficult to detect, understand and properly mitigate. "This has stopped being a compliance issue and is now a very real business issue for us," said a CAE at a Dutch manufacturer. Another CAE said their organisation was reassessing ties with good suppliers in Israel because of potential political activism.

In this volatile, complex environment failing to quickly identify and assess risks has become a risk in its own right with potential financial penalties, activism attention and reputational damage. The introduction of the European Union's Corporate Sustainability Due Diligence Directive (CSDDD) should provide an opportunity to improve visibility and transparency in the supply chain by 2029, one CAE said.

Such complexity demands good scenario planning. "You cannot create a strategy without scenario planning because there are too many variables, so it is fundamental to think through what could go wrong, how you deal with it at a fundamental level," the Dutch CAE said.

Creating the right scenario planning process was critical. For example, teams needed a diverse group of people involved to avoid group-think, discover blind spots and challenge core assumptions.

MACROECONOMIC AND GEOPOLITICAL UNCERTAINTY

Businesses also needed to develop a clear definition of successful outcomes. But too often scenario planning was myopic. “We might think quite short term about war and those things in front of us we have the data for, but we often don’t extend beyond that to the next possible set of events that could arise from our scenarios,” a CAE from a UK-based insurer said. “There is a risk we are constantly planning, but never prepared.”

Shifting political landscape

Given that an estimated three billion people will have voted across the globe by the end of 2025 – including in the European Union, France and the UK in 2024 – uncertainty is at a high as changing political agendas could affect the business landscape. And with misinformation and disinformation technologies on the rise, influencing political discourse and potentially undermining the legitimacy of newly elected governments has become a geopolitical risk, according to the World Economic Forum.

As a result, long-term planning for major capital investments has become hugely challenging, CAEs said. Potentially, incoming governments could increase taxes to fulfil election pledges and meet high debt repayments – leading to a higher-inflation economy over the next three years. Money remains tight with CAEs rating financial liquidity and insolvency a top 10 risk in this year’s survey – with 27% rating it as a top 5 risk.

Risk assessments needed to be better integrated into strategic decision making, CAEs at the roundtable said.

Businesses were reinforcing and rehearsing disaster recovery processes and CAEs had also experienced a sharp rise in informal calls from audit committee members and executives to brainstorm key risks. “As a non-executive director, I encourage my CAEs to be bold and brave and be prepared to be involved in the decision-making process by, for example, challenging the assumptions of our decision-making processes,” said a non-executive director and business professor in the Netherlands in an interview for this project.

MACROECONOMIC AND GEOPOLITICAL UNCERTAINTY

Most CAEs have moved to dynamic audit planning where, for example, the annual plan comprised a list of potential risk themes, but the actual assurance assignments were chosen on a quarterly basis. Others had increased investment in audit automation to free up time for dealing with more “nebulous assurance” where data was not available – and to provide more real-time controls testing and monitoring.

Keeping the board informed is a must. “CAEs must ensure that the board receives a summary of emerging risks over the next two to three years that shows how those threats align with and impact upon the strategic goals of the organisation,” a CAE at a Spanish insurer said in an interview for this project. “Only companies that have a vision of where the world is going are likely to survive.”

"CAEs must ensure that the board receives a summary of emerging risks over the next two to three years that shows how those threats align with and impact upon the strategic goals of the organisation”

How internal auditors can help organisations

1. Provide assurance that processes for identifying and mitigating risks that potentially impact multiple parts of the business are properly integrated throughout the enterprise
2. Provide assurance that the organisation’s resilience efforts work at a strategic level so that issues such as business model disruption are considered along with, for example, capital requirements and cybersecurity
3. Assess whether the organisation makes adequate use of stress testing in key risk areas
4. Provide assurance that scenario planning processes are robust, wide-ranging and long-term enough to adequately capture possible emerging risk scenarios
5. In preparing for the introduction of CSDDD, provide assurance that organisations have visibility over the entire business value chain to identify and mitigate potential second and third order risks
6. Provide assurance that emerging risk processes are regularly reported to the board and assessments are aligned with the strategic direction of the business

CLIMATE CHANGE, BIODIVERSITY AND ENVIRONMENTAL SUSTAINABILITY

Boosting resilience through compliance

The scale of regulatory compliance is helping organisations strengthen environmental sustainability efforts but with unpredictable physical factors, transition strategies prove tough to implement.

One third of CAEs in the Risk in Focus 2025 survey said that climate change, biodiversity and environmental sustainability was a top 5 risk – 15% of those said it was their number one threat. Since last year's survey, it has lost its place as the fastest growing risk to digital disruption, new technologies and AI, but 50% of CAEs said it would be a top 5 risk by 2028. Significantly, internal audit effort is expected to double from 20% who said it was a top 5 area of effort to 40% who said it would be by 2028.

33% of respondents said **climate change, biodiversity and environmental sustainability was a top 5 risk.** 15% said it was their top priority.

Reporting readiness

With the first annual reports to be published under the Corporate Sustainability Reporting Directive (CSRD)[12] due in 2025, CAEs at the roundtable said it was their number one area of focus. Few felt ready – even in industries with strong existing environmental regulations over, for example, chemical manufacturing and industrial effluence. The much broader scope, detail and mandatory nature of CSRD has made it a major compliance effort. From that perspective, all organisations have immature data processes, at least in part of their operations, and few have deep experience of co-ordinating efforts across the enterprise at this level of detail. While UK businesses align more with Task Force on Climate-related Financial Disclosure (TCFD), all organisations doing business in Europe follow CSRD.

CAEs at the roundtable continued to provide assurance over data gathering and testing efforts in the first and second lines and to conduct gap analyses. This year, there was added focus on bringing the rigour associated with mature systems and controls surrounding financial reporting to climate-related reporting.[13]

"The key step is for the organisation to integrate those climate-related data into the existing data architecture – and into core systems applications," a CAE at a Spanish bank said in an interview for this project.

[12]CSRD mandates that companies must comply with European Sustainability Reporting Standards
[13]See COSO's 2023 guidance Achieving effective internal control over sustainability reporting

CLIMATE CHANGE, BIODIVERSITY AND ENVIRONMENTAL SUSTAINABILITY

"That has to be done with the same quality of controls you find around financial data because they now have the same level of importance."

A CAE at a Spanish energy company told the roundtable that he was providing design assurance to management: "We go in early before the process starts to work to make sure the key controls and the key points are attended to so that we do not have a problem with compliance in future," he said. In addition, he said that he was trying to ensure the business was in good shape before the organisation's external verification exercise – a mandatory requirement under CSRD. But few CAEs said they had been involved in providing assurance over their organisations' double materiality risk assessments[14] because of the volume of more basic compliance hurdles facing them in 2025 – a trend that is most likely to have changed by 2029.[15]

This lack of data maturity is likely to impact the reporting cycle. A CAE at a German chemicals conglomerate said that his business – like many others – would provide limited assurance under CSRD in 2025.[16] Most likely, the business would miss the reporting deadline. "Maybe we will be able to produce unaudited key figures in time and a month later release audited figures," he said. "But investors typically want audited financial statements so that may impact access to capital markets."

Physical risk

Since Europe has the fastest-warming continent globally, CAEs are increasingly auditing business continuity and resilience with an eye to whether the risk management around physical assets is accurate and robust. In fact, 33% of survey respondents ranked business continuity as a top 5 risk, putting it in 7th place in the rankings.

At the roundtable, CAEs said they often integrated physical risks related to climate change into regular assurance assignments.

[14]Double materiality is a key plank of CSRD and a recommendation of the IPCC's sixth assessment report to help companies take measures to help prevent global emissions rising by 1.5 degrees Celsius or more, and reduce the adverse social and biodiversity impact of their activities
[15]European Union's Corporate Sustainability Due Diligence Directive (CSDDD) comes into effect from 2029 putting more focus on ESG in the supply chain
[16]Businesses have 4 years to move from limited to reasonable assurance.

CLIMATE CHANGE, BIODIVERSITY AND ENVIRONMENTAL SUSTAINABILITY

For example, the CAE of a Swiss chocolate business said, “At a local level, internal audit looks at how well the business is dealing with flooding and heavy rain. Across the group, risk management uses geo-data software to look at climate change models and simulations.” Most organisations used modelling and artificial intelligence to help identify emerging risks. For example, one business taking part in the qualitative research used GPS satellite programs to assess the impact of future floods |on 12,000 stores; another used satellite images to assess levels of deforestation across its operations and those of its suppliers.

Overall, asset management strategies in the first and second line were being put on a more solid basis with risk managers, for example, developing enterprise-wide dashboards to better monitor risks. “For banks, physical risk is mostly a credit risk,” a CAE from a bank in the Netherlands said, “and the longer-term view on physical resilience is a major factor in how we provide loans.”

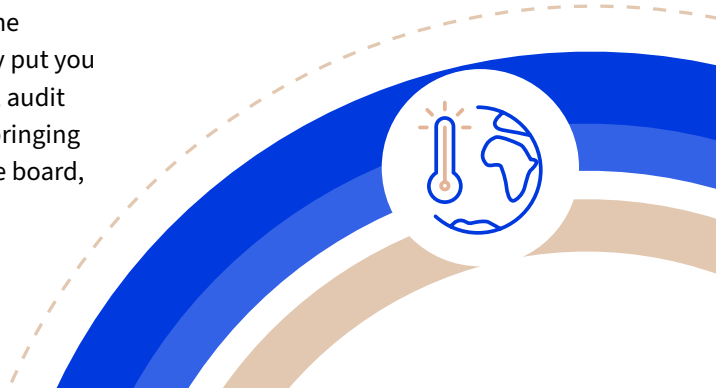
While organisations clearly benefit from advanced technologies in risk assessment and evaluation, a CAE working in the Swedish financial services sector said that organisations had limited opportunity to assess the accuracy of third-party, AI-powered climate-assessment tools. “Different AI companies will use different assumptions in their modelling, which potentially opens us up to a form of third-party risk,” she said.

Identifying obvious disruptive events does not guarantee the business’ longer-term sustainability, a board advisor at EFRAG (a body that drafts reporting standards for the European Commission), said in an interview for this report. He explained that wine production in France, Italy and Spain had fluctuated unexpectedly recently, with little chance of accurately predicting future trends. “That demonstrates that issues such as extreme heat and the availability of water can effectively put you out of business,” he said. “Internal audit has a key strategic role to play in bringing those issues to the attention of the board, ensuring they are considered in resilience and business continuity plans, and that monitoring and controls are in place.”

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

Transition risk

Transitioning to a greener economy presents both a huge business model risk and opportunity. Organisations are changing the composition of their portfolios, replacing or relocating suppliers to cut carbon footprints, and launching new products.



CLIMATE CHANGE, BIODIVERSITY AND ENVIRONMENTAL SUSTAINABILITY

While the European Union's Climate Law committed to achieve net zero by 2050 under the Green Deal, hitting those targets is not certain – and policies could change because of the new composition of parliaments in the European Union, France and the UK following elections in summer 2024.

With uncertain transition timescales, accurate forecasting is difficult – and planning specific, long-term remediation action involves balancing conflicting strategies, a head of risk at a German energy group at the roundtable said. "You have greater transitional risks when you are transitioning and physical risk reduces; but bigger physical risks when you are not transitioning," he said. "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." In fact, a report by the UK Financial Reporting Council said that its review of Task Force on Climate-related Financial Disclosure (TCFD) disclosures revealed that companies struggled to explain transition plans, which often lacked clear targets and metrics.

While CAEs said that regulation such as CSRD and TCFD would help tighten controls around their own processes, relying on 3rd party evaluations of investment products could be a risk.

It also presented a market risk as "companies are finding a new window through which to launch climate products, insurance and other financial vehicles that we did not see even a year ago," said a CAE at a Swedish financial services business. "That creates a client risk for those who do not believe your products are in line with their appetite. It is becoming a major strategic risk for us." In addition, financial services groups wishing to launch green and sustainable bonds and socially responsible investment products could face charges of greenwashing – making the need for the right levels of transparency high.[17]

In addition to flagging up areas where their organisations need to allocate additional resources, CAEs are also helping businesses ensure processes are in place to identify cost-savings in the supply chain and helping assess technology risks where expectations of the scalability of new solutions is untested.[18]

> "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"

[17]Regulation is increasing in this area in some jurisdictions. See, for example, the UK's anti-greenwashing guidance.
[18]For other useful strategies, see Chartered IIA's 2021 Harnessing internal audit against climate change risk.

CLIMATE CHANGE, BIODIVERSITY AND ENVIRONMENTAL SUSTAINABILITY

How internal auditors can help organisations

1. Provide assurance that the business is on track to elevate the detail and quality of controls around climate-related data and integrate it into core systems applications
2. Provide assurance that the organisation is doing adequate materiality risk assessments
3. Advise management in assessing the impact of late reporting under CSRD on investor relations and reputation risk and provide assurance that processes are in place to manage those risks
4. Provide assurance that the business is adopting long-term, strategic planning for physical assets and that risks are properly assessed and monitored
5. Assess the extent that technologies to assess physical risk or investments in green products are transparent in light of potential green-washing and reputational risk
6. In preparing for the introduction of CSDDD, provide assurance that organisations have visibility over the entire business value chain to identify and mitigate potential second and third order risks
7. Provide assurance that risk management is focusing on operational resilience and contingency planning for the uncertainties associated with transition risk planning

ABOUT RISK IN FOCUS

For the past nine 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 2025 involved a collaboration between 19 European Institutes of Internal Auditors, spanning 20 countries including Albania, Armenia, Austria, Belgium, Bulgaria, France, Germany, Greece, Hungary, Ireland, Italy, Luxembourg, The Netherlands, Norway, Poland, Portugal, Spain, Sweden, Switzerland and the UK.The highest number of European countries involved so far.

The survey elicited 985 responses from CAEs across Europe. Simultaneously, five roundtable discussions were organised with 48 CAEs on each of the risk areas covered in the report. In addition, we also conducted 11 one-to-one interviews with subject matter experts that included CAEs, Audit Committee Chairs and industry experts to provide deeper insights into how these risks are manifesting and developing.

ECIIA

IIA Austria

Albania

The Institute of Internal Auditors Armenia

Institute of Internal Auditors Belgium

IIA Bulgaria

IFACI Elevating Impact

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 Luxembourg

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