
2026
RISK IN FOCUS
Hot topics for internal auditors
Read more
ECIIA

CONTENTS

Contents

EXECUTIVE SUMMARY:

As Europe faces another once-in-a-lifetime shock, organisations must adapt strategic objectives and innovate to take advantage of emerging opportunities and markets.

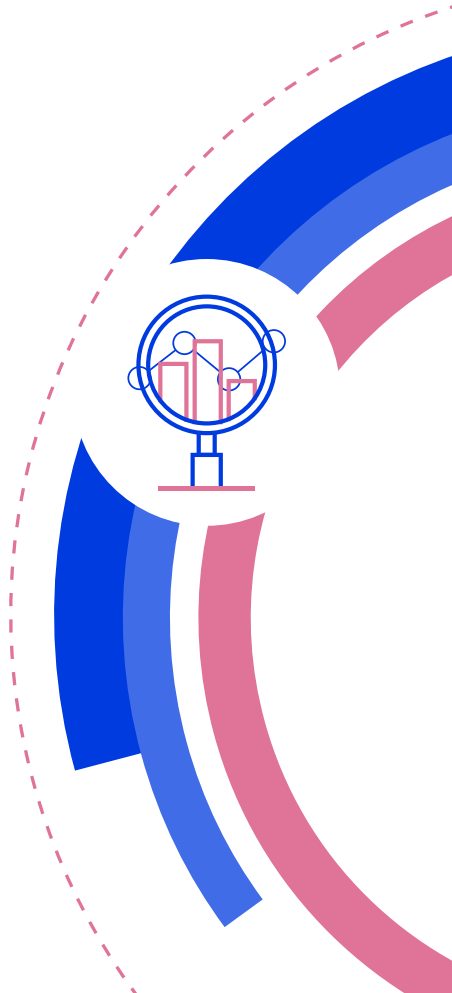
While the impact of the COVID-19 pandemic was fading in 2025, conflicts continued in the Ukraine and Gaza. Added to those events, the US administration's unpredictable use of tariffs in trade negotiations worldwide, gave Europe its "third 'once-in-a-lifetime' shock … in fewer than five years," according to Citigroup.

That has injected geopolitical and macroeconomic uncertainty into every aspect of the threat landscape for Risk in Focus 2026. Yet those risks join extreme weather, fresh deregulatory initiatives, the rapid spread of Artificial Intelligence (AI) and persistent cyberthreats in an inter-connected array of pressing issues that demand urgent action. As the global economy heads to its weakest levels since the financial crash of 2008, according to the World Bank Group, organisations will be tackling those problems with limited budgets.

Risk in Focus 2026 draws on a survey of 879 CAEs, 5 roundtable events with 44 participants and 10 one-to-one interviews to map the key challenges, organisational responses and internal audit's remit over five hot topics:

Key Points

- **Macroeconomic and geopolitical uncertainty** was in joint 4th place for 2026 together with **changes in laws and regulations**. CAEs participating in the report agreed that the threat permeated every other risk category. The way that global trade wars, tariffs and sanctions affected changes to laws, cyber threats, market conditions and AI were high on organisations' agendas, according to a special question in this year's survey
- **Digital disruption, new technology and AI** continued to be a growing risk, moving from 4th to 3rd place in 2026. CAEs said that developing strategies for fast-moving generative AI systems was particularly challenging and expressed concern over the potential for vendor lock in



Contents

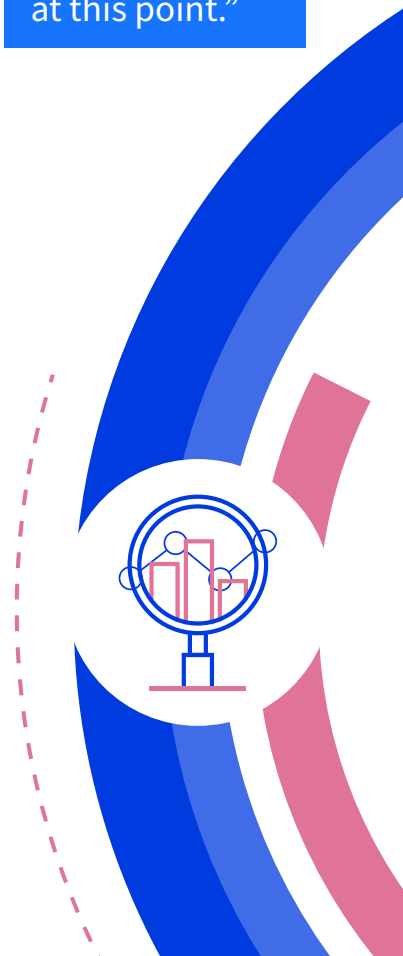
- **Cybersecurity and data security** remained the biggest overall risk. CAEs said the increased technical sophistication of attacks as represented a constantly "emerging risk," and some were preparing for the advent of post-quantum encryption
- **Human capital, diversity, talent management and retention** kept its position as the 2nd largest threat to organisations in 2026. Fears of deskilling because of AI, and an inability to attract and retain the right skills, were major concerns
- **Climate change, biodiversity and environmental sustainability** fell two places to 10th place this year, despite the worsening impact of extreme weather in Europe. CAEs at the roundtable expressed frustration over regulatory uncertainty shaped by changing political attitudes in Europe and globally. Only 24% predicted it would be a top 5 area of audit focus by 2029 – down from 40% who said so last year

Given the growing complexity and uncertainty of the risk landscape, organisations are struggling to set and execute strategies. Nowhere is that more evident in the field of AI, with developments in generative AI in particular outstripping the ability of organisations to understand how programs could disrupt business models and strategies. "It's hard to develop a strategy more than two or three quarters out," a CAE from a Dutch financial services company said, "so agility and being adaptive is key at this point."

Traditional methods for assessing and mitigating risk impacts in all categories are being tested. This year's survey results saw the top 4 risks after cybersecurity bunching closer together than at any other time (at between 45%-48%). This suggests that many CAEs see their organisations' core risks as relatively equal because they have become more interconnected making risk management especially challenging. An audit committee chair provided one example for this report: his UK financial institution's worst-case scenario calculations of the impact of US tariffs were wide of the mark. CAEs must provide assurance that planning and decision-making processes were fit for such purposes if organisations are able to rethink, regroup and change course at speed, he said.

This will be particularly important as the competitive landscape continues to change. New global players are rising rapidly, entering European markets and challenging the dominant players. **Market changes, competition and changing consumer behaviour** ranked 7th in the survey at 32%. For those that chose this risk, 23% said it was their top priority. Pressure is coming from start-ups, such as Chinese car manufacturer BYD and AI business DeepSeek, which are making significant inroads. More will follow.

"It's hard to develop a strategy more than two or three quarters out, so agility and being adaptive is key at this point."



Contents

If European businesses are to thrive in this complex environment, they will need to become nimbler and more focused on exploiting and creating opportunities. CAEs are adapting to provide services to match the speed of change. One said that demand for internal audit advisory services now took up over half of his annual plan – up from about 20% over the past 2 years. Others said boards and management wanted CAEs to share knowledge on emerging and inter-connected risks, offer constructive challenge and provide advisory services on the viability of new commercial initiatives so that they could proactively exploit emerging opportunities.

CAEs can play a pivotal role in supporting the future success of their organisations. Their mission is to "strengthen the organisation's ability to create, protect, and sustain value by providing the board and management with independent, risk-based, and objective assurance, advice, insight, and foresight," according to the 2024 IIA Global Internal Audit Standards. Evidence from this report shows that the best internal audit functions are already fulfilling that role – and it provides a roadmap for those others who have already started on that journey.

METHODOLOGY

In the first half of 2025, a quantitative survey was distributed among chief audit executives (CAEs) by 14 European Institutes of Internal Auditors, spanning 15 countries: Austria, Belgium, France, Germany, Greece, Hungary, Ireland, Italy, Luxembourg, The Netherlands, Norway, Spain, Sweden, Switzerland and the UK. The project was conducted in partnership with the European Confederation of Institutes of Internal Auditing.

This year, 10 in-depth interviews were conducted with CAEs, audit committee chairs, non-executive directors and industry experts from a range of 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 44 participants in total, comprising mostly of CAEs but also including Audit Committee Chairs, Non-Executive Directors, academics and industry experts.

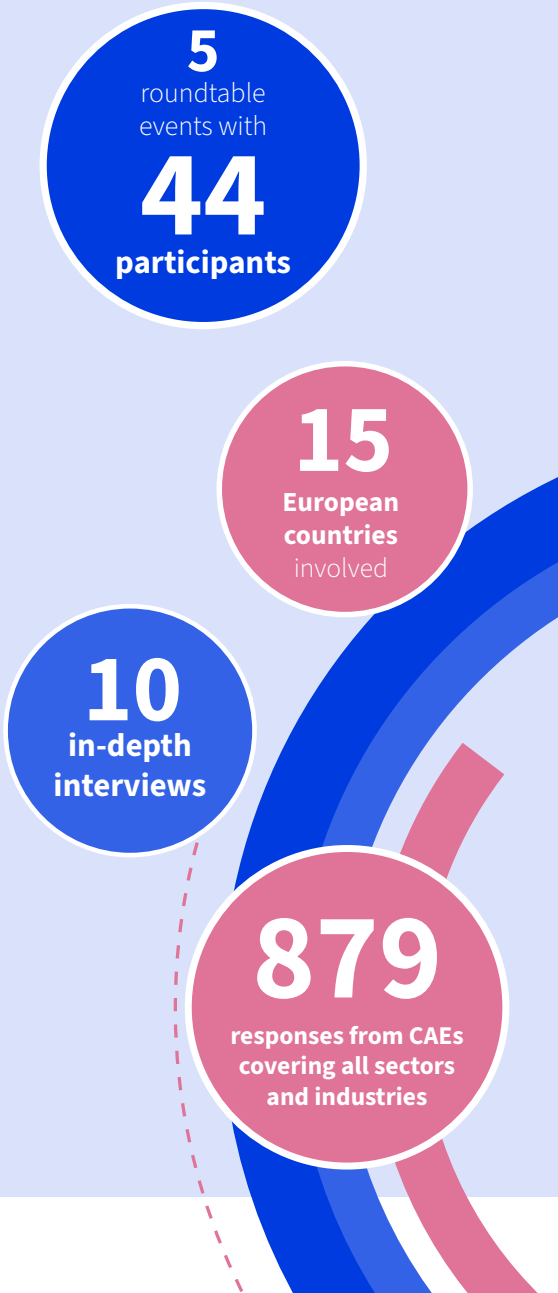
The analysis in this report was determined by the quantitative survey results, guided by the one-to-one interviews and enriched by the roundtable events. All participants contributed on the condition of anonymity.

This year marks the 10th anniversary of the report. The current format builds on the success of a change in approach since Risk in Focus 2023. Rather than focusing only on the 5 top-rated risks, the report takes a deeper look into areas of pressing importance to internal audit and its stakeholders.

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 and risk management, along with other assurance and governance professionals.

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

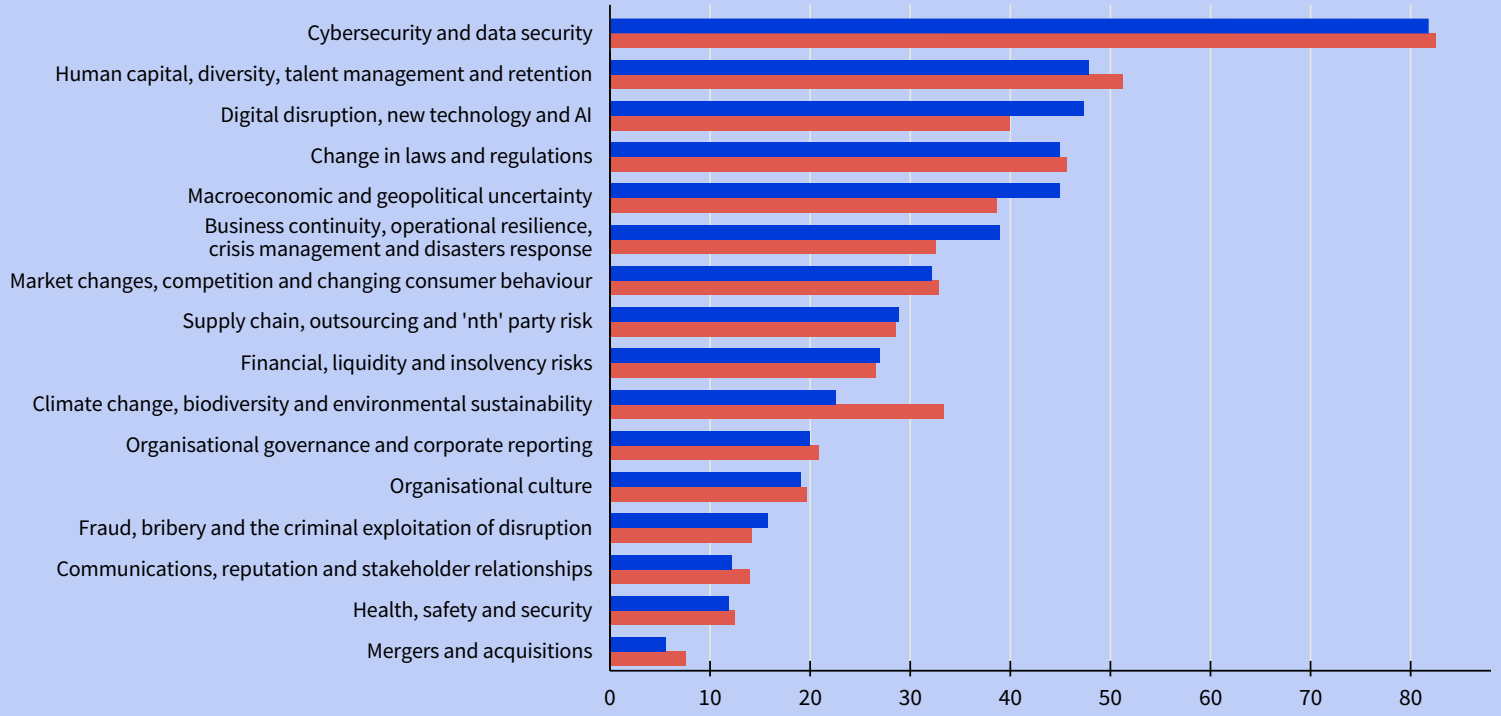
A Board briefing is also available so that CAEs can engage stakeholders in conversation about key survey findings. In addition, there will be a series of follow-on roundtables providing input for a series of webinars at the end of 2025.



Key survey findings

What are the top five risks your organisation currently faces?

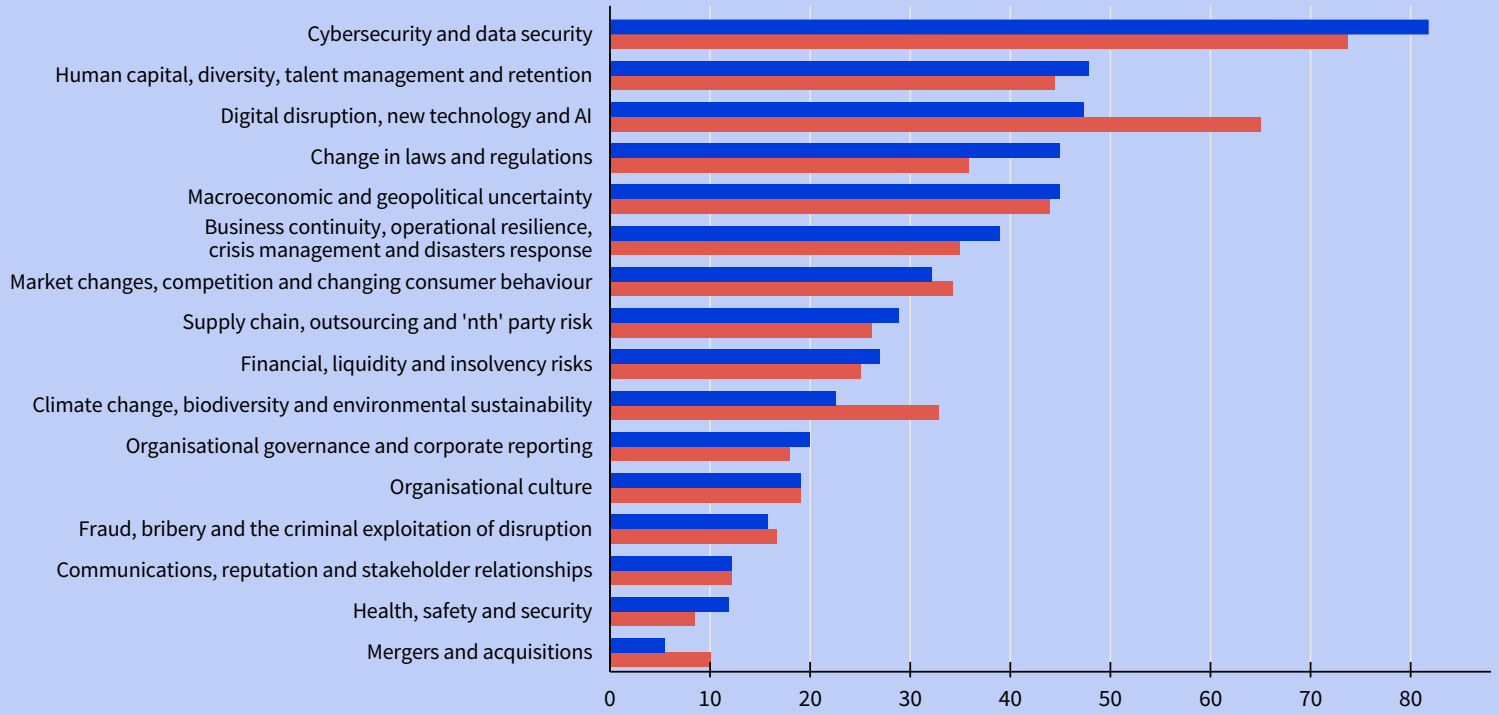
Cybersecurity still dominated the risk rankings, but the top 4 risks beneath bunched closer together suggesting that CAEs see their organisations' core risks as carrying relatively equal weighting due to their interconnectedness.



Looking ahead

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

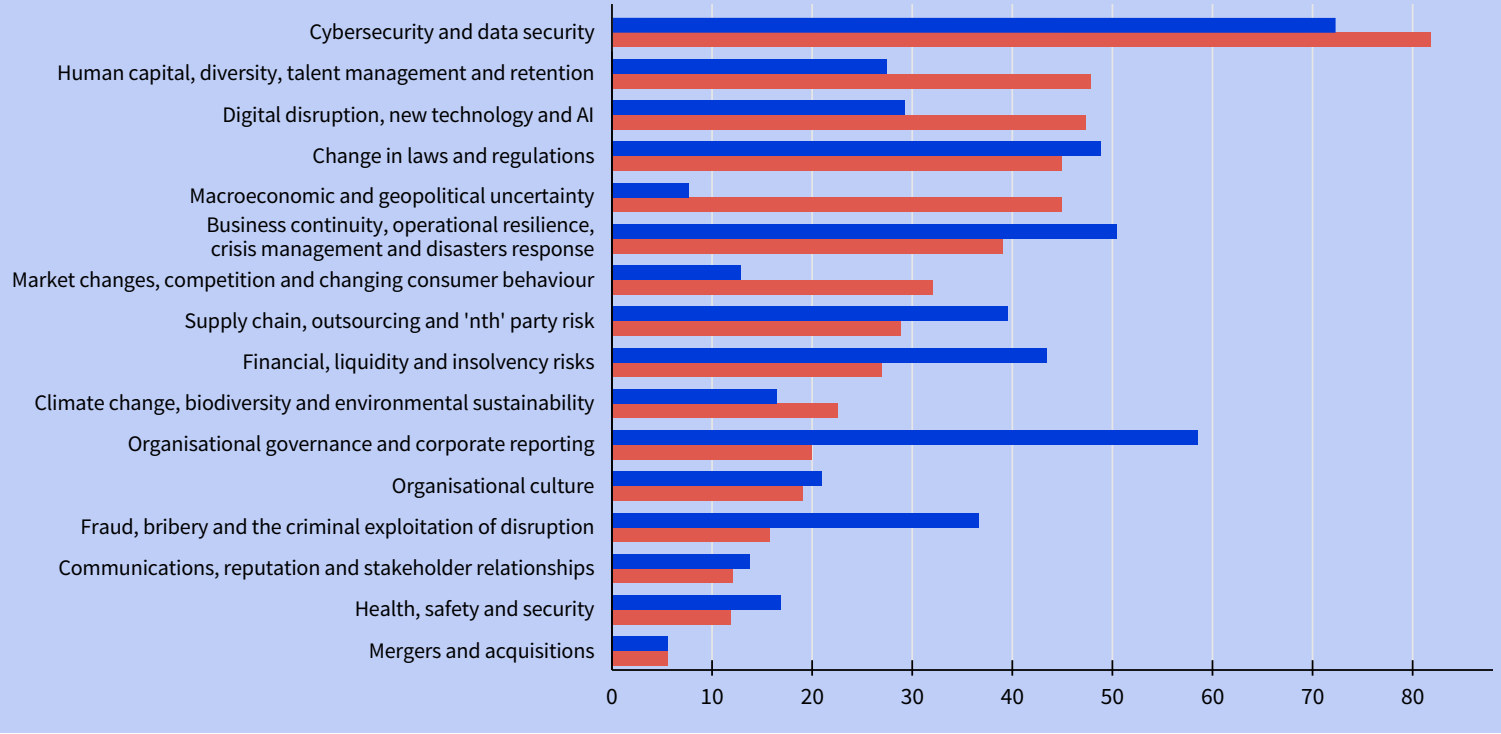
Digital disruption is expected to continue its upward trajectory, but climate change is expected to remain a lower-rated threat despite the worsening impacts of extreme weather.



Risk priorities vs. audit's focus

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

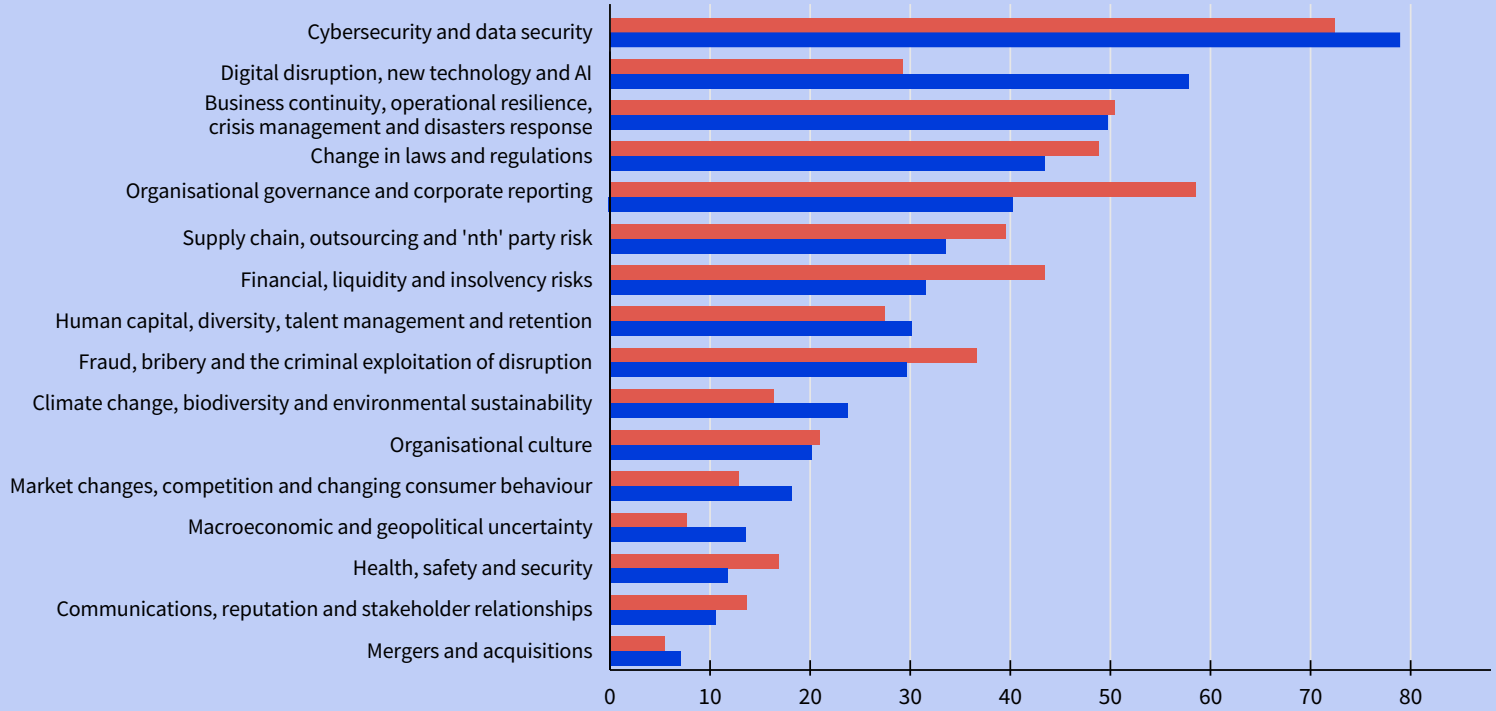
Internal audit functions spent most time on cybersecurity, organisational governance and business continuity, but efforts lagged strategically important risks such as digital disruption and human capital risk.



Looking ahead

What are the top 5 risks you expect internal audit to spend the most time and effort addressing 3 years from now?

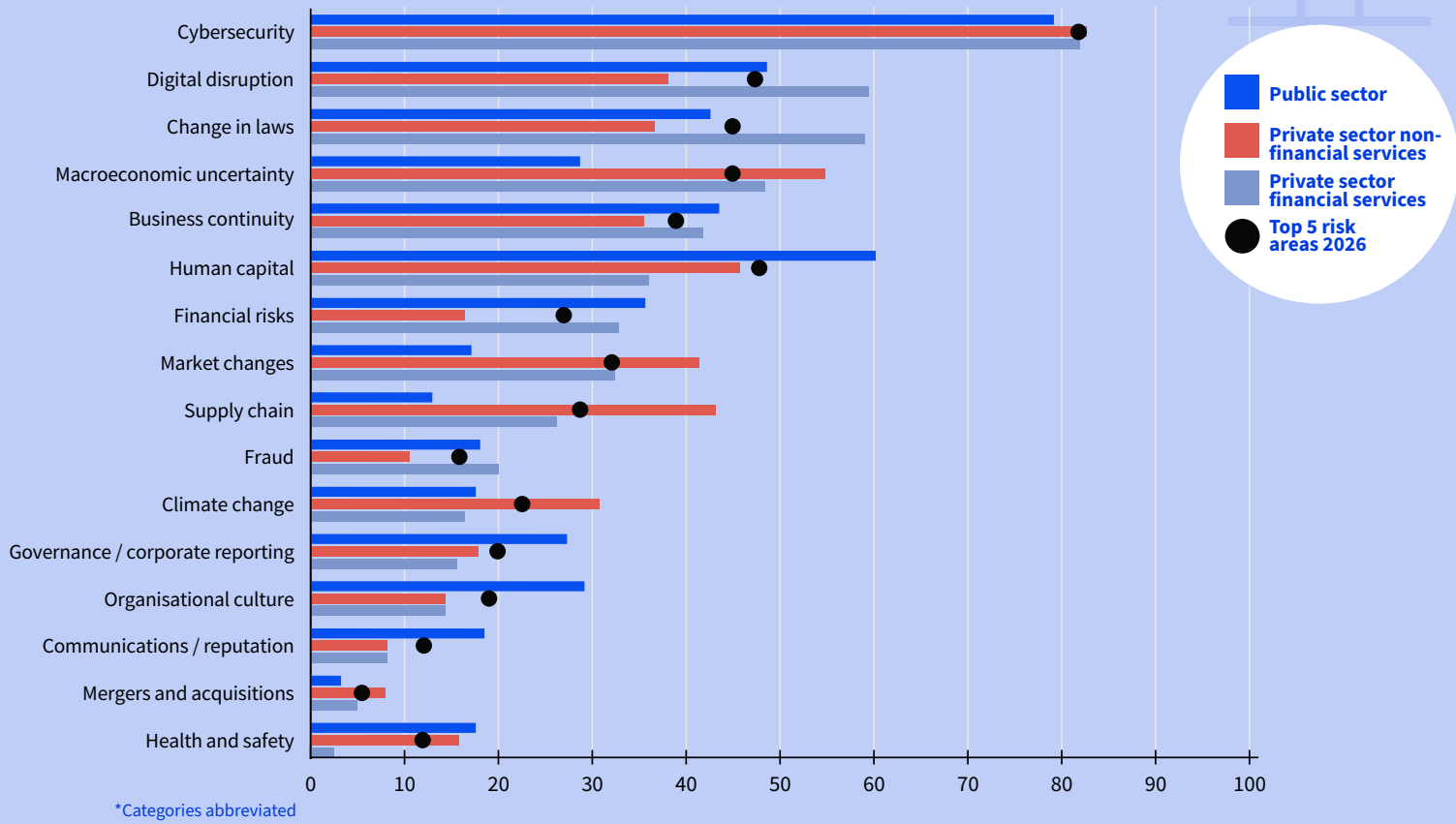
Almost twice as many CAEs expect digital disruption to be a top five area of focus in 3 years' time and effort on climate-related activities will rise only modestly.



Key survey findings

Top 5 risks by sector

Unsurprisingly, all 3 sectors rated cyber security and data security as their organisation's highest risk. However there are differences across the remainder. The public sector had human capital as its second highest, whereas financial services had macros economic and the private sector had digital disruption.

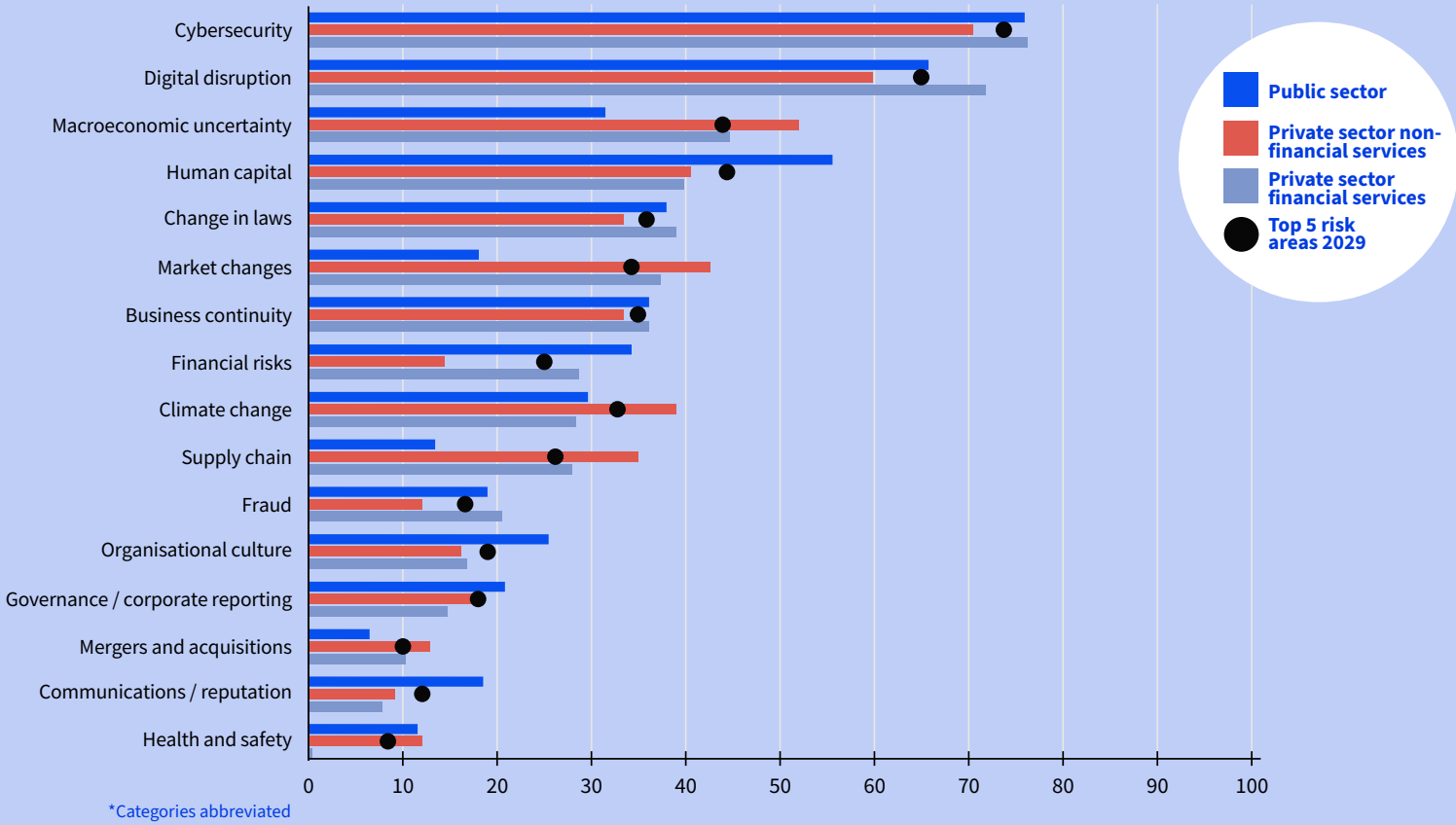


*Categories abbreviated

Looking ahead

Top 5 risks by sector in 3 years time

Cybersecurity again is expected to be the top risk in 2029, with digital disruption, new technology, and AI expected to be in second place across all three sectors.



*Categories abbreviated

MACROECONOMIC, SOCIAL AND GEOPOLITICAL UNCERTAINTY

Creating upsides from ambiguity

US tariffs, ongoing wars and political uncertainty are leading organisations to reassess their strategic goals.

When US President Donald Trump named 2 April 2025 "liberation day", countries around the globe faced huge tariff increases on goods exported to the country. As the initial promise of 90 deals in 90 days has faded, unpredictability has become the new norm, according to the BBC. Tariffs on European exports to the US (except for the UK) – its largest export market – were still ongoing during this project.

Together with wars in Ukraine and Gaza, these factors helped place geopolitical and macroeconomic uncertainty 4th in this year's Risk in Focus survey – joint with changes in laws and regulations. Nearly a third (32%) of those who selected this issue said it was their number one priority, second only to cyber security at 37%. Only 8% of CAEs said they spend significant time specifically auditing or consulting on the issue with most focusing on the potential impacts of such risks on their organisations.

CAEs were asked in the survey how government policy changes related to this topic were impacting their organisations. They said the greatest effects were on significant changes in laws and regulations (65%), perhaps reflecting concerns about tariff increases and the weakening of environmental regulations.

Fragility of global trades

The past 5 years has exposed the vulnerability of global trade flows. The OECD estimates that structural changes to trade that would normally take 5 years took place in one during the pandemic outbreak of 2020. Huge disruption to trade with Russia followed invasion of Ukraine; and $600 billion worth of goods were held up globally when a single ship – the *Ever Given* – blocked the Suez Canal in 2021.

US trade tariffs could have greater and more long-lasting impacts, according to participants at a roundtable on the topic. A CAE at a European drinks manufacturer estimated that it could cost millions of dollars – or upwards of a billion – to redesign supply chains and build new markets. "By the time we have done that the landscape may have completely changed," he said. This has increased uncertainty over decisions to change strategic direction or make significant investments.

MACROECONOMIC, SOCIAL AND GEOPOLITICAL UNCERTAINTY

Because of higher levels of disruption, a CAE at a manufacturing business in Italy said that internal audit's first role was to assess and confirm that the company had adequate risk management processes around its supply chains to detect and assess the changing risks. He was also working with his compliance and legal functions to gain audit rights to third parties to assess the strength of their risk management processes – although negotiations were complex, he said. In the survey, half of internal auditors said that business continuity and operational resilience was a top 5 area of effort – the 3rd-highest category in this year's survey and up one place from last year.

Further geopolitical tensions between the US and China could also complicate trade. CAEs said that if, for example, the US sanctioned specific businesses (as with TikTok in 2024), it could make it impossible or uneconomic to deal with those suppliers.

"Organisations need to be specific about how expected changes to the macro and micro political environments are likely to impact them," a board member of a global financial services business based in the UK said at the roundtable.

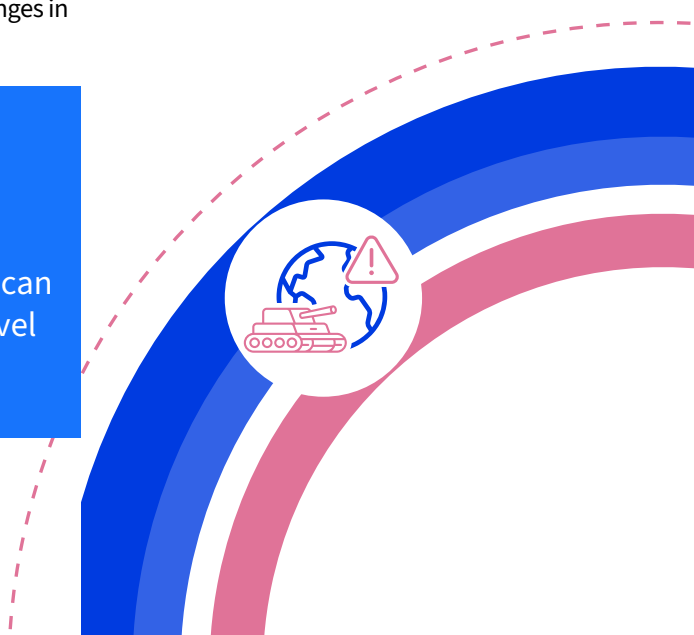
"You need to compartmentalise it, understand what you are trying to fix and what you can control, and decide the level of risk you want to take."

Agility was key, he said, which meant that those threats should be incorporated into the risk framework of the organisation to speed up responses to changing events. At some organisations, geopolitical risk management frameworks had become more structured and formalised, CAEs said. If potential risk levels became too high, second-line functions needed to implement mitigation actions quickly. Internal auditors had a key role to keep up to date with rapid changes in the field.

"You need to compartmentalise it, understand what you are trying to fix and what you can control, and decide the level of risk you want to take."

Downturn and financial instability risk

Global growth is expected to be at its weakest level since the economic and financial crash of 2008, according to the World Bank Group. Financial liquidity and insolvency risk was up one place to 9th place in the survey, with 27% of CAEs saying it was a top 5 risk. For those who chose this category, 30% said it was their number one risk.



MACROECONOMIC, SOCIAL AND GEOPOLITICAL UNCERTAINTY

A CAE at a global European drinks company said that any sharp rise in export tariffs in its key markets could reduce the spending power of customers – hitting sales, profits and cash flow. "We have a big, booming business in places in Asia that have been hit hard with tariffs," he said. "If the trade barriers for them to export to the US significantly slows growth in those economies, we will feel it because we rely heavily on the purchasing power of the growing middle classes."

The key is to be able to cope with fast-moving risks. The CAE at the drinks company said the percentage of his audit plan devoted to traditional assurance assignments had dropped from about 80% to 45% over the past couple of years. During the past year he had provided advisory services on a greater number of projects, including the business' approach to innovation, product launches and marketing.

"I try to put myself as much as possible in an assurance role, so I am not being negative, but I want to know whether the business division is sufficiently in control of achieving its operational or strategic objectives given the resources, product levels or financial budgets in place," he said.

CAEs at the roundtable said organisations must avoid being too reactive and properly consider potential upside risks. Ensuring sound decision-making was key, including providing assurance around those processes. A UK risk and internal audit consultant at the roundtable said that CAEs needed a seat at the top table to provide supportive challenge. "One of the sub-components of strategic risk is groupthink," he said. "CAEs should be asking what arrangements has the board, or management, made to ensure that such thinking does not contaminate the strategic formation process."

The CAE from one Italian manufacturer said his organisation had invested significantly in leadership development, so that they are "ready and able to detect issues and take proactive steps to grasp opportunities". This was particularly important as major competitors were quickly developing a European presence, such as the Chinese electric battery business EVE Energy and tech giant Alibaba.

Political and regulatory uncertainty

CAEs at the roundtable said that domestic politics in Europe was an increasing concern because swings to and from established political parties was becoming greater and less predictable. For example, the UK Labour Party swept to a historic victory and the right-wing Reform Party unexpectedly placing 2nd in the popular vote. In addition, many French voters surprised pollsters by opting for the left-wing New Popular Front alliance, which became the largest single party in the French government.

MACROECONOMIC, SOCIAL AND GEOPOLITICAL UNCERTAINTY

Those swings could create more regulatory uncertainty as domestic political agendas clash with international business practices. According to the CAE of a Spanish aviation business interviewed for this report, organisations increasingly face a "regulatory puzzle" comprising a growing patchwork of national and supranational frameworks with diverging priorities and timelines. Divergence in climate-related regulation was one example, see Climate change, biodiversity and environmental sustainability.

"The challenge today is not only the continuous change in rules across multiple jurisdictions, but also the feeling that these rules could be diverging significantly, which makes long-term investment decisions particularly difficult," he said.

The business, he explained, decided to ensure that it complied with European standards across the global enterprise, not only because it is based on the continent, but because in areas where it promotes, for example, (digital) operational resilience, doing so can lead to competitive advantage.

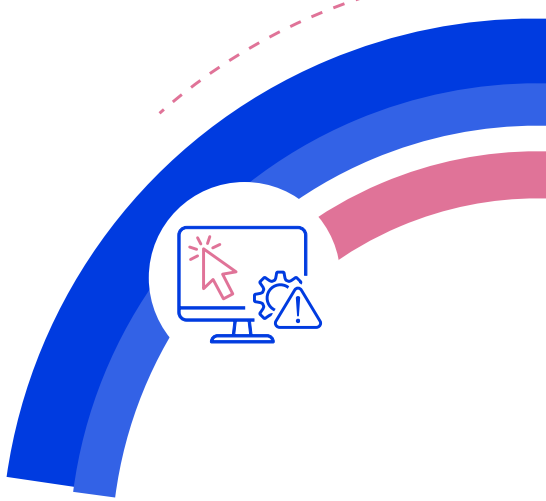
In addition, trying to fragment compliance efforts to meet every local regulation would be too costly. One strategy has been to have organisational data in the cloud to push some of the compliance issues around data localisation onto that provider, he said.

How internal auditors can help organisations

1. Provide assurance that issues related to geopolitical and macroeconomic uncertainty are properly reflected in the organisation's risk assessment and responses to these are developed and tested
2. Assess how well the organisation has broken down the overall risk category into issues that are specifically relevant to the business' objectives and strategy
3. Provide assurance that board-level and management-level decision-making processes have all necessary input and are free from groupthink and other biases, and that the board has the appropriate level of diversity of experience and training
4. Engage with management on innovation and commercial opportunities and reflect on how well strategies match risks and available resources and budgets, and ensure risks are understood and mitigated
5. Provide assurance on the design and effectiveness of third-party risk management processes with a focus on continuity, quality and compliance
6. Provide assurance on business continuity and short and long-term resilience

DIGITAL DISRUPTION, NEW TECHNOLOGY AND AI

Balancing risk and innovation



Organisations are striving to develop AI strategies when the potential benefits and risks of those technologies are unclear.

Investment into AI in Europe is rocketing, partly in an attempt to create US-style technology giants, a failure recognised by the 2024 Draghi report on EU competitiveness. For example, in February 2025 the European Commission announced the creation of InvestAI, a €200 billion public–private partnership, which aims to develop the region's technology infrastructure. The analyst Statista estimates that Europe's AI market will grow 305% to a value of €215 billion by 2031.

But the region is also under pressure to loosen its regulatory environment to boost investment. Companies such as SAP and Siemens have called existing data protection legislation "toxic for the development of digital business models." As the European Commission reviews its stance, it must balance competition, investment and protection to make its ambitions a reality.

Digital disruption, new technology and AI continued to rise in the Risk in Focus survey, moving from 4th to 3rd place in the risk rankings in 2026 (it ranked 6th in 2024). It was CAEs' 8th-highest area of focus – moving up two places from 2025 – a trend CAEs expect to continue: 58% said it would be a top 5 priority in 3 years' time, second in importance only to cybersecurity and data security.

In addition to generative AI, other technologies are developing quickly, including quantum computing (see Cybersecurity and Data Security below). So, while businesses are rightly focused on exploiting today's technologies, they must be scanning the horizon for emerging technologies that have potential, strategic importance.

Vendor lock-in and third-party management

The generative AI landscape is very dynamic, making it impossible to predict which vendors will become predominant and that will provide the best service. Becoming locked-in to a vendor can limit flexibility and increase security threats: technical problems, changes in ownership or a decline in competitive features can all be risks.

A senior IT internal auditor at an energy company based in Spain said at a roundtable on the topic that his company had adopted a multi-cloud approach when using large language models (LLMs) Different AI models could be switched between cloud systems to test performance and build up expertise in the IT team.

DIGITAL DISRUPTION, NEW TECHNOLOGY AND AI

The company also used popular productivity tools with built-in AI features and compared the results to test performance. Other organisations are creating ventures using European vendors to localise services and reduce dependence on US companies, according to one CAE.

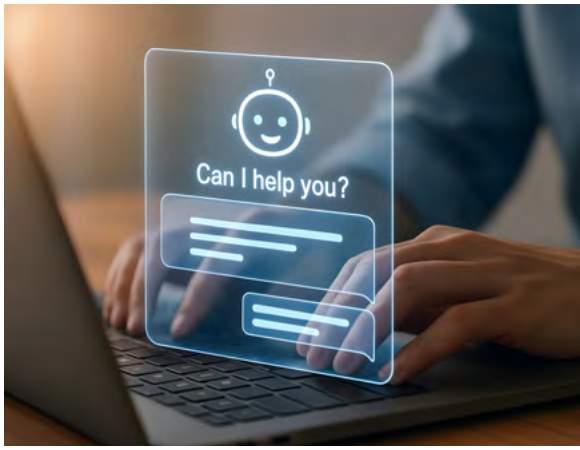
Previous issues of Risk in Focus show that trying to get access rights to audit large technology businesses can be difficult, but not impossible. Negotiations should be a key part of onboarding vendors, as should governance, risk management and controls for third-party management (see IIA's Third-Party Topical Requirement). This year, a CAE at a large Swedish bank said his organisation had joined forces with other European finance groups to gain audit access rights to large US technology companies. "It has been quite successful," he said, "but you have to have a lot of resources to put in the negotiation team." Organisations must evaluate the costs and benefits of different means of getting assurance from their providers: the International Standard on Assurance Engagements or System and Organisation Controls statements are frequently used alternatives.

Uncontrolled adoption of generative AI

If managing suppliers can be difficult, retaining control over how AI is used within the business can be equally challenging – especially for LLMs, which are freely available and can leak corporate data. Anecdotally, one audit discovered pre-approval processes were ignored in 90% of cases, according to a CAE interviewed for the report.

Unlike with mature cloud technologies, organisations feel constantly overtaken by technical innovations in generative AI, making an approach difficult to define. "It's hard to develop a strategy more than two or three quarters out," a CAE from a Dutch financial services company said, "so agility and being adaptive is key at this point."

Companies are experimenting with AI strategies to strike a balance between rapid adoption and risk. "The new technology is quite a radical innovation, so it is very hard to imagine how much value your organisation can get out of it," the CAE at a German aviation business said. "We decided to make a lot of these tools available with safeguards around the data and then let people get on with it." Because it can be difficult to understand whether AI adoption could help the business achieve its strategic objectives, it had also set up a multidisciplinary centre of excellence to review the results, identify opportunities and strengthen its governance processes.



DIGITAL DISRUPTION, NEW TECHNOLOGY AND AI

A CAE at a pharmaceutical business in Italy said it had taken a more cautious approach. It only allowed the use of generative AI models where more conventional AI processes already existed, so that experimentation only happened in areas with mature data governance. Managers in excluded areas were frustrated, he admitted. "We are also investing a lot in AI literacy, so, as the technology evolves, people understand the risks around cybersecurity, confidentiality and exfiltration – but they also appreciate how and where we can use generative AI most effectively," he said.

CAEs were reviewing the data security and governance processes around new AI implementations (see IIA's guidance on auditing AI) – some had conducted pre-audits to help management consider the potential risks and controls.

A CAE implementing AI into his own processes said that as well as being properly documented, audit tests done using generative AI needed to be assessed to see whether the same input prompts created the same results and, crucially, whether there was a human in the loop to review the main outcomes of those systems. "Internal auditors should see generative AI as a super-smart intern that should be constantly under review. That's because it looks smarter than it actually is and, as an intern, you have to recheck whatever it produces," he said.

Understanding AI decision-making

Since AI systems often operate as "black boxes", their decisions can be difficult to interpret and audit – and may even fall foul of provisions on the responsible use of AI in the European AI Act. "If your business has a lot of its processes effectively hidden in opaque artificial intelligence models where decisions take place in a 'black box', that is worse than vendor lock-in, it is close to corporate suicide," a CAE at a Spanish financial institution said in an interview for this project. Since even organisations with high-levels of IT maturity may be unable to provide an adequate level of assurance over the results, he added, regulatory approval for their use could be problematic.

In addition, a CAE from a major European travel business said that teams tasked with implementing AI needed to have a deep understanding of the business and be aligned with the organisation's corporate culture: "We need highly skilled IT people in our team, but they need to be on board with the corporate culture and understand what are we really doing to make sure that the work that they perform is actually in line with our core values." Management must also be trained to understand the outputs from AI – as must internal audit functions if they are to provide assurance on its outputs.

"If your business has a lot of its processes effectively hidden in opaque artificial intelligence models where decisions take place in a 'black box', that is worse than vendor lock-in, it is close to corporate suicide."

DIGITAL DISRUPTION, NEW TECHNOLOGIES AND AI

AI regulation and compliance

CAEs agreed that European technology regulations such as the Digital Services Act could make their organisations uncompetitive. The EU has already dropped its planned AI Liability Directive and further deregulation may follow because of political pressure from the US. In 2025, at the AI Action Summit in Paris, US Vice President JD Vance said the US would not tolerate rules that slowed AI innovation in US companies. CAEs said that it was difficult to balance data protection compliance in global organisations with rapidly deploying new AI systems. Internal audit functions had a key role to play in keeping track of developments and in informing the board how those changes would affect corporate AI strategies.

How internal auditors can help organisations

1. Provide assurance that the organisation's horizon scanning processes take account of emerging technologies and regulatory changes that may have potential, strategic relevance to the business
2. Assess whether the organisation's AI strategy is flexible enough to take advantage of fast-moving technical developments and avoids the risk of vendor lock-in
3. Provide assurance that governance and risk management processes around AI innovation are effective and in line with its strategy and compliant
4. Provide assurance that AI procurement processes are robust and, if relevant, work with other organisations to expand third-party assurance rights
5. Provide assurance that the processes around assessment of the effectiveness of AI results are robust and interdisciplinary
6. Assess the maturity of AI literacy across the enterprise (including the boardroom), and assess the business and cultural literacy of AI technicians

CYBERSECURITY AND DATA SECURITY

Defending against sophisticated attacks

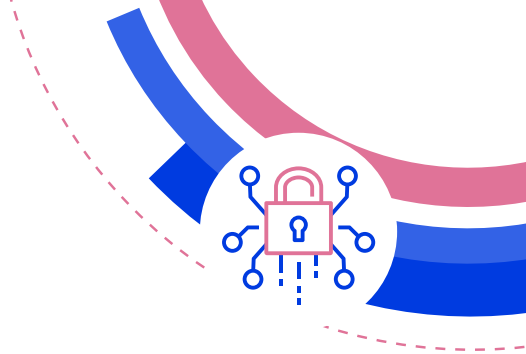
While some organisations may be overstating their exposure to cyberattack, increasingly sophisticated methods are a key concern, as is the future switch to quantum cryptography.

Cybersecurity continued to dominate the risk rankings with 82% of CAEs scoring it as their most important threat. Of those choosing this category, 62% said it was their organisation's 1st or 2nd priority. Internal audit effort seemed well aligned to this risk with 72% of respondents saying it was their main area of focus. And just as it has been the top risk for organisations since Risk in Focus began, CAEs expect it will still be so in 3 years' time.

Cybersecurity continued to dominate the risk rankings with **82%** of CAEs scoring it as their most important threat

But is this ranking and level of focus justified? In early 2025, UK retailer Marks & Spencer's (M&S) cyber defences were breached by a ransomware attack costing the company an estimated £300 million for the year. Such headline-grabbing events are supported by surveys showing that, as digitalisation and AI adoption increase in speed, companies create more potential vulnerabilities for hackers to exploit.

Yet perhaps cases such as M&S stand out because they are exceptional. The average cost of a breach in 2024 was a little under $5 million, according to a study by IBM and the Ponemon Institute. In fact, research shows that measured as a percentage of revenue, cyber exposure has dropped every year since the height of the COVID-19 pandemic in 2022 when it stood at 2.84%; in 2025, the figure was 1.32%.



CYBERSECURITY AND DATA SECURITY

Analysis of these figures by the online magazine GRC Report said that this decrease was due to organisational maturity, better negotiating skills during ransomware attacks, lower regulatory fines, reduced reputational risk and having countermeasures built into third-party systems. In other words, 3 years' worth of effort and investment in cyber defences has paid dividends.

The magazine also suggested that the discrepancy between survey results – such as those produced in Risk in Focus – and the real-world analysis of breaches could mean that "when executives and others answer surveys about cyber risk, they are thinking of the level of risk without countermeasures". But given the high level of investment and attention this risk has received over the past decade, that may not reflect an organisation's current exposure to the risk. That is not to say cybersecurity risk is not a major threat nor that emerging post-quantum cryptography could be hard to quantify; it may even be the top threat for many organisations. However, CAEs should assess whether organisational risk assessments consider the maturity of its cyber defences.

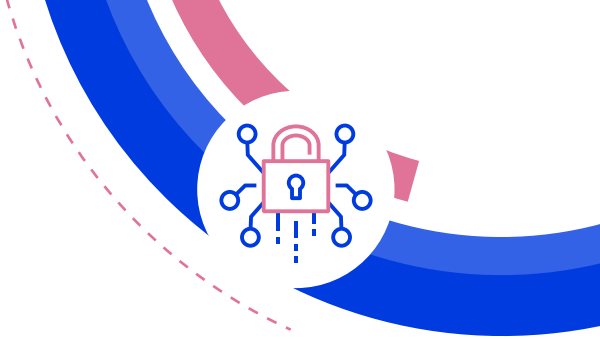
Sophisticated external threats

Every year the risk landscape evolves. In 2025, the velocity of attacks continued unabated and CAEs at the roundtable on the topic described an increase in the sophistication of hacking threats. Of particular concern were authentic-looking phishing emails generated by AI, deepfake attacks on key personnel and, especially, the successful targeting of multi-factor authentication (MFA) systems. The widespread assumption among organisations was that MFA represented a gold standard in cyber defence. It requires users to verify their identity through multiple methods. Yet research reported in the online magazine Cyber Security News showed that hackers had bypassed MFA by targeting the processes around the technology. "Security teams are finding these attacks especially challenging to detect as they appear as legitimate authentication workflows in security logs," it said.

Organisations have also seen a rise in advanced, persistent threats – long-term, complex, hard-to-detect attempts to steal sensitive data or disrupt operations. During an interview, the CAE at a European automotive parts manufacturer said his organisation had been targeted twice by such attacks. "They aim to get into your systems, penetrate them very deeply and stay there," he said. "They want to steal resources [and] data and disrupt operations. It is a significant concern and one we have identified as an emerging risk." Such attacks are often associated with state-sponsored groups, although not exclusively.

Digitalisation, AI systems and talent

Now that most customer and supplier transactions take place through integrated, digital interfaces, successful hacks are potentially catastrophic. Instead of simply strengthening cyber defence systems, some organisations are restructuring their digital infrastructures.



CYBERSECURITY AND DATA SECURITY

As well as implementing the company's strategic cybersecurity plan, the automotive parts business has also begun a parallel segmentation plan to cut connections between factories and between internal systems. "If attackers manage to enter, let's say, the finance function in a factory, they cannot also access operations models or logistics, for example, so the segmentation is designed to reduce the severity of an attack and improve our resilience," he said.

The CAE at a European nuclear power business said that his organisation isolated backups of all data to prevent ransomware attacks. It regularly tested whether its operations could be rebuilt from scratch from those backups following any attack. While many organisations back up data to secure cloud providers, hackers have more recently attacked backup infrastructure – making it a key area for CAEs to provide assurance over.

Generative AI and other AI systems are not only expanding the risk surface but are also boosting threat detection efforts.

Most CAEs said that their organisations utilise AI for detecting potential attacks within their systems. Third-party suppliers, in particular, have integrated generative AI within their programs to help, for example, with detecting sophisticated phishing emails and malware.

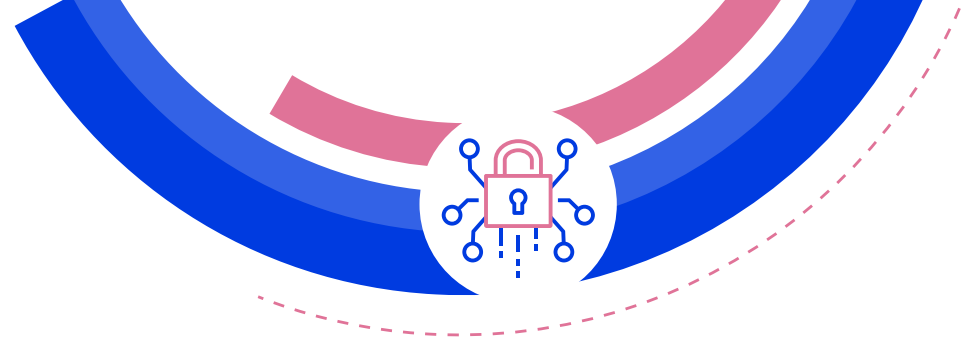
Yet with the growth of state-sponsored threats, organisations must ensure legacy AI systems – such as some spam filters – are not open to infiltration, said the CAE at an academic institution in the Netherlands. She said it was also important to keep track of how geopolitical events may affect the availability and suitability of cybersecurity software from countries such as China given heightened tensions between it and the US. When the Kasperksy virus scanner was banned by the Dutch government several years ago, for example, implementation was instant. Organisations' corporate IT inventories must detail the countries of origin and ownership structures of vendors if they are to be able to respond quickly to such sanctions.

Several roundtable CAEs said that they had focused more of their efforts this year on third-party assurance audits and cybersecurity governance reviews – responsibilities that are explicitly dealt with by the IIA's Cybersecurity Topical Requirement and related guidance (see Digital disruption, new technology and AI).

Yet accelerated AI adoption had increased skills shortages and organisations' dependence on third-party providers – often depriving businesses of key in-house cyber and digital expertise. See Human capital, diversity, talent management and retention on digital skills risks.

Preparing for Q-Day

Hackers are stealing data for the day they get hold of quantum computers – known in the industry as Q-Day. The rapid development of AI – especially over the past 12 months – has led to projections by experts such as Bill Gates that quantum computers could be a reality within 3 to 5 years.



CYBERSECURITY AND DATA SECURITY

While timelines are still uncertain, in 2024 the US Department of Commerce's National Institute of Standards and Technology published its first set of encryption algorithms designed to withstand cyberattacks from a quantum computer. The US National Security Agency released its resources in 2025.

During the roundtable, a CAE at an insurer based in Austria said that quantum computing could break current encryption methods and undermine the security foundations of many business-critical systems. As quantum computing evolved, it could create additional IT vulnerabilities. His main concern was that hackers would obtain such a computer and that "after this pivotal moment, there may no longer be sufficient time for an orderly migration to quantum-resistant algorithms, posing a significant operational and security risk to organisations," he said.

His first internal audit on the issue in 2026 would focus on cryptography and key management. First, he said that it was critical that organisations revisited the basics to follow fundamental, best-practice cybersecurity processes. Second, he would assess how well the corporate group was preparing for the transition to quantum cryptography, a transition that would take a year or more to complete. "This topic does not appear to be in the spotlight at the moment," he said, "so I see it as our responsibility as internal auditors to shine a light on it."

How internal auditors can help organisations

1. Provide assurance that cyber risk assessments fully consider new cyber threats and the maturity of the organisation's defence processes
2. Provide assurance that the security processes, such as those around multi-factor authentication, are up to date and effective
3. Assess how well the organisation's cyber defence strategy has considered the possible segmentation of physical sites or IT programs to reduce the risk of corporate takeover by hackers
4. Provide assurance that the organisation is able to restore backups and that the backup processes and infrastructure are secure
5. Provide assurance that the organisation's risk management processes take account of geopolitical threats that may impact the business' core programmes
6. Provide advisory services to the business on the transition to quantum cryptography and keep the board informed of the potential risks of this transition to the organisation

HUMAN CAPTIAL, DIVERSITY, TALENT MANAGEMENT AND RETENTION

Companies restructure their workforce around AI

Organisations are working to realign their workforce strategies with their developing AI capabilities, but struggle with talent shortages and high staff turnover.

Europe is suffering from a skills shortage, according to a European Commission action plan designed to help organisations tackle the problem. It said that around one-fifth of Europe's working-age population was inactive and there were 42 occupations with talent shortages – from skilled manufacturing and building staff to software, chemical and environmental engineers. "Labour and skills shortages are expected to continue rising over the coming decades, predominantly thanks to demographic change and the increase in the demand for workers with specific skills," it said.

Staff turnover is high and lengths of tenure low, according to the HR professional body CIPD. On average, for UK workers, 3 in 10 workers leave their organisations each year. Average tenure (22%) was between 2 and 5 years. Hiring and retaining staff in such an environment has become tough and simply making the workplace more attractive is not enough. Human capital's strategic importance is growing as technology transforms business skills and career structures.

This helps explain why human capital issues have ranked 2nd in this survey since 2023, only making it as a top 5 risk during the pandemic. However, human capital issues ranked only 9th in terms of internal audit effort, with just 27% saying it was a top 5 area of focus.

Human capital issues have ranked

in this survey since 2023, only making it as a top risk during the pandemic.

HUMAN CAPITAL, DIVERSITY, TALENT MANAGEMENT AND RETENTION

AI displacement and de-skilling risk

"The impact of AI on businesses is moving far quicker than anyone could have imagined, so it is now starting to interfere with the design of specific white-collar jobs," a UK training consultant and non-executive director said in an interview for this project. "It is causing real stress in the workplace, but competitive pressures for efficiency mean that organisations often ignore emotional reactions among staff that they need to deal with."

Any AI transformation strategy must contain a HR strategy that tackles such issues if the expected productivity benefits are to be fully realised, he said. CAEs at the roundtable on the topic said that their organisations are pursuing two strategies: improving communication with staff and providing more transparency on the impact of AI on the business and employees. Yet many organisations can only develop short-term strategies because of an incomplete understanding of the potential impact of AI technologies on operations and on careers (see Digital disruption, new technology and AI). Even new AI jobs, such as prompt engineering, can quickly become obsolete as the technology develops.

A CAE at an HR and payroll business in Belgium said that, in the medium term, the loss of experience and knowledge to AI could be a bigger problem. "We have a large population of payroll consultants who deeply understand their roles because of the knowledge and experience they learnt as juniors doing basic work," she said. "We are really struggling to understand how senior people in future will get these skill sets and how we can restructure those careers with AI."

Despite concerns over succession and skills disruption, upskilling and reskilling was a major focus. Many organisations were implementing certification programmes in AI for staff in all departments to improve AI competencies and data analysis capabilities, CAEs said.

HUMAN CAPITAL, DIVERSITY, TALENT MANAGEMENT AND RETENTION

They were helping their organisations identify gaps in digital literacy and using their enterprise-wide remit to share knowledge. Some organisations were collaborating across business units to provide training.

Strategic accountability and governance gaps

Strategic HR planning was identified as a weakness in last year's report. In most businesses, HR planning focused mainly on headcount needs (66%) that covered a one-year period (61%), according to a survey of HR professionals by the analyst Gartner. Such organisations were stuck in tactical and reactive cycles with processes often misaligned with business-critical initiatives, it said.

CAEs at the roundtable said that some of their organisations lacked top-level ownership, involvement and oversight of strategic human capital risks. Responsibility often remained fragmented – split ineffectively between HR and business leaders, according to the CAE at a German manufacturer in an interview for this report.

On a strategic level, a CAE from a financial institution in the Netherlands said: "Internal audit should be able to judge how well the talent strategy of the board matches the organisational vision and to act as a sparring partner for the board to provide constructive challenge."

In addition, well-structured governance processes could bring together leaders from across the business to focus on their organisation's strategic needs, CAEs at the roundtable said. Organisational governance and corporate reporting was the second biggest area for internal audit effort in this year's survey, suggesting the efforts of CAEs in human resources may be higher than the headline figure. Specific assignments included talent gap analysis and providing assurance around strategic HR planning processes. But some said that where formal plans and procedures were lacking, they were unable to provide effective assurance. In those cases, providing advisory services was the best way to add value, CAEs said.

Remote and hybrid working and employee well-being

While the security and access management issues of remote working are no longer a key risk, supervision of staff, reviewing work quality, communication and co-worker collaboration have remained problematic in some organisations, CAEs said. Since flexibility is a baseline expectation of many employees, organisations are grappling with how to maintain workplace cohesion and creativity without full office attendance. Those who get a firm grip on this issue could poach hard-to-find talent and stem attrition.

HUMAN CAPITAL, DIVERSITY, TALENT MANAGEMENT AND RETENTION

The CAE at one business in Spain said the company required on-site attendance for some tasks: since the headquarters were not in a major city, recruitment and retention were challenging. Adopting a hybrid model with different attendance requirements for different functions had helped.

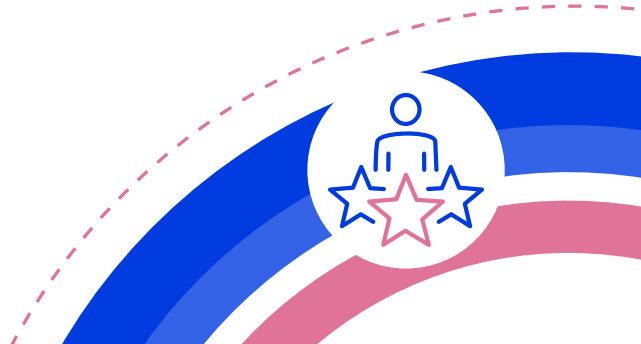
Organisations were also struggling to effectively deliver employee well-being and promote psychological safety programmes. Those create an environment in which people feel able to voice contrary opinions, contribute new ideas and discuss mistakes in order to learn lessons. During the qualitative interviews, several participants made unprompted comments about the need to strengthen diversity of thought at organisations.

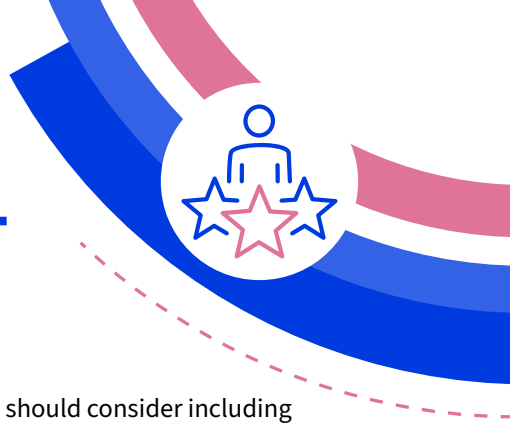
Where these initiatives were poorly documented and lacked specific controls, CAEs said assurance could be hard to provide. A CAE at a European bank recommended internal auditors review HR policies and procedures on, for example, psychological safety to see how well they were communicated and whether they were implemented consistently.

In addition, internal audit findings from other assignments that touched on these issues, such as from whistleblowing procedures, could be collated and assessed. This would facilitate themed assurance reporting for the audit committee and senior management. Where the function lacked skills, it could call on external, professional help, she said.

Pay transparency directive

During 2026 the EU's Pay Transparency Directive is expected to come into force in different European jurisdictions. Companies will need to report the gender pay gap across their organisations. That will require both detailed reporting on pay gaps and a justification for any pay differences for equal work. In addition, organisations could need to re-evaluate the way they structure their rewards and benefits – in some cases, making significant changes to compensation frameworks and grading systems.





HUMAN CAPITAL, DIVERSITY, TALENT MANAGEMENT AND RETENTION

"CAEs can help their organisations by assessing existing pay structures, data availability and reporting capabilities," said the CAE at a bank in Greece. That would highlight discrepancies between current practices and the directive's requirements and provide recommendations to address related reputational, legal and operational risks associated with non-compliance.

In addition, internal audit functions could validate the accuracy and completeness of employee data in such areas as job classifications, pay levels and gender. They should also evaluate whether systems can generate the required reports and disclosures and collaborate with HR to ensure robust analytics for pay gap analysis.

"CAEs should consider including pay transparency compliance in the internal audit plan and tracking progress against the compliance roadmap to flag delays or issues," she said. Benchmarking the company's practices with industry peers could help identify best practices and areas for improvement.

How internal auditors can help organisations

1. Provide assurance that emerging AI strategies and HR strategies are aligned with each other and with the organisation's objectives, and that processes exist to keep them synchronised
2. Provide advisory services on whether governance systems for strategic HR planning are appropriate and that responsible individuals are clearly identified
3. Assess whether the organisation understands the impact of AI systems on existing roles and how far the organisation risks losing key organisational knowledge and skills in the transition to greater digitalisation
4. Provide assurance that career planning and progression routes take account of the impacts of digital disruption and that opportunities are clearly communicated to staff
5. Assess the level of psychological safety and, where behavioural and formal procedures are lacking, recommend improvements
6. Provide assurance that the organisation's compliance efforts for the EU Pay Directive are on track and that the relevant data is both accurate and complete

CLIMATE CHANGE, BIODIVERSITY AND ENVIRONMENTAL SUSTAINABILITY

Seeking sustainability during regulatory uncertainty

While most CAEs agree that the scope of European ESG regulation is too broad, many worry that the benefits that the reporting regime promised will be lost.

Climate change, biodiversity and environmental sustainability dropped from 6th to 10th place, making it the biggest mover in the survey. In addition, while 16% of respondents said it was a top 5 area of internal audit effort (down from 20% in 2025), only 24% predicted that would be a top 5 areas of effort in 3 years' time. That compares with 45% who said it would occupy significant internal audit time last year.

From an environmental impact perspective, the fall is illogical. Last year, the European Environment Agency published its first ever risk assessment for the region, which showed higher temperatures and flooding had posed an increasing risk to lives and livelihoods in recent years. "When applying the scales of severity used in the European climate risk assessment, several climate risks have already reached critical levels," the agency said. The OECD said that positive climate action in the region would lead to an uptick in global GDP by 0.2%, whereas "avoided economic losses" could reach 13%.

While the benefits of climate-friendly strategies look obvious, politically the world is moving in the opposite direction. For example, in 2023 the UN climate summit in the United Arab Emirates ended with a historic decision to "transition away from fossil fuels". Yet in 2025, US President Donald Trump's slogan "drill, baby, drill" was the headline catchphrase heralding a huge drawing back from green policies in the US and potentially in many other countries, according to reporting by the BBC.

CLIMATE CHANGE, BIODIVERSITY AND ENVIRONMENTAL SUSTAINABILITY

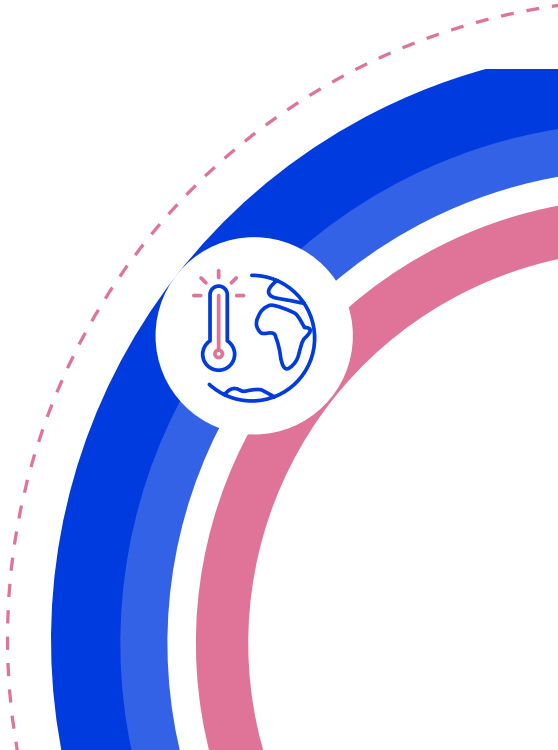
Europe is at a crossroads. A global leader in environmental, social and governance regulation and reporting, the political will to continue on this path may be floundering. In 2024, former Italian prime minister Mario Draghi published The Future of European Competitiveness. It outlined a bleak future in which the region's social structures would fail without radical productivity improvements. Bemoaning an inability to capitalise on the region's world-leading innovations in clean technologies, the report backed a 25% cut in ESG reporting obligations for organisations (50% for small and medium-sized enterprises). Whether Europe can build its economy along green lines while others are increasing their reliance on fossil fuel technologies is a vital but open question.

"This uncertainty in policy direction in Europe and the fact that climate-related risks have too long a timescale compared with, say, cybersecurity or geopolitical risks mean that it has fallen down the agenda in many boardrooms," a CAE at a global travel business in Germany said for an interview for this report. "Companies are looking at the business cases for investment, or regulatory compliance risk, and are struggling to see more than 2 or 3 years ahead. They don't worry whether a supplier in another country could be under water in 20 years' time."

Increasing regulatory uncertainty

The European Union's Omnibus simplification package has signalled a significant easing of regulatory requirements. Relaxing rules in the Corporate Sustainability Reporting Directive (CSRD), the Corporate Sustainability Due Diligence Directive and European Sustainability Reporting Standards could transform the regulatory landscape. The Commission expects to shave off €4.4 billion in compliance costs, but the proposals were met with frustration by CAEs at a roundtable on the issue.

"My real fear is that the omnibus deregulation and the Trump effect will lead to companies failing to tie sustainability and climate-related goals into the business plan and deter them from creating a green vision for the organisation," a CAE from an insurer in Sweden said. "If we don't have a set of explicit goals against which to measure our performance, we will see a lot of wishful thinking but little concrete action."



CLIMATE CHANGE, BIODIVERSITY AND ENVIRONMENTAL SUSTAINABILITY

Many CAEs agreed that the provisions of CSRD were complex. A CAE at a retail and wholesale business in France said that CSRD had been positive in bringing ESG issues to the board's attention, but complexity had been a major challenge. The breadth of CSRD had also made creating enough quality data against which to measure ESG goals difficult, a CAE at a financial services institution in Sweden said. "Environmental risks are very difficult to calculate, but it is crucial to have good data in order to aid decision-making, especially in areas where business goals may conflict with environmental risk," she said.

The majority had already completed compliance efforts and believed new uncertainty over important elements of the regulations, such as carbon reporting rules and double materiality, could outweigh projected deregulatory benefits. While compliance was still critical, CAEs should help organisations focus on the bigger picture, according to a partner in sustainability at a major European consultancy. "The priority for a CAE in this area is to help the board understand the changing landscape, but more importantly clarifying and assessing risks to the business model is a key role for internal audit however the regulations may change," he said.

Double materiality

Double materiality assessments (DMA) required under CSRD were a challenge for many companies. Organisations must assess the short-to-long-term impacts of their activities and value chains on the people and environments in which they operate. At the same time, they must report on the material, financial impacts and opportunities for the organisation from those external risks.

Frameworks such as those developed by the Taskforce on Nature-related Financial Disclosures and the Committee of Sponsoring Organisations of the Treadway Committee are designed to help organisations get a grip on those inter-relationships.

CLIMATE CHANGE, BIODIVERSITY AND ENVIRONMENTAL SUSTAINABILITY

They also help strengthen data quality and risk management techniques to support long-term sustainability efforts. Additional guidance is available from EFRAG.

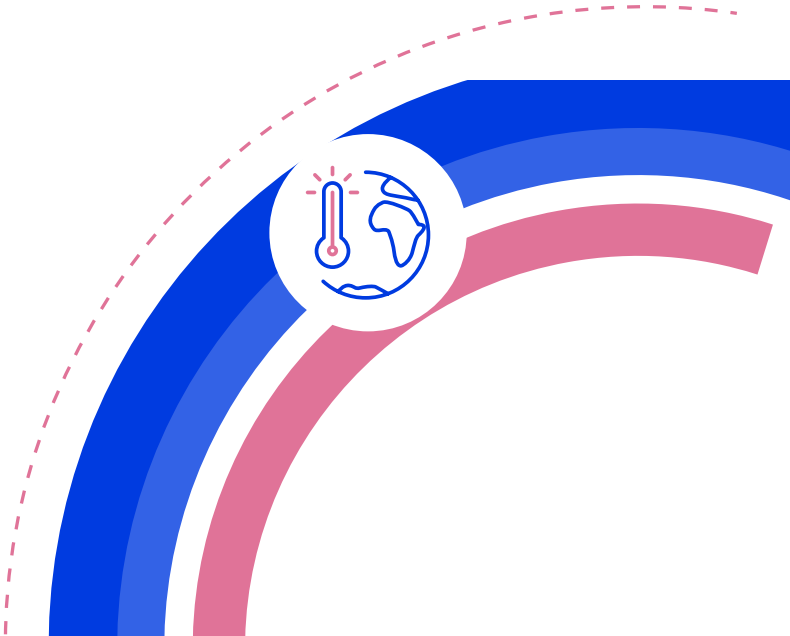
"Double materiality assessments are really important for internal auditors because they help us understand which topics to focus on," a CAE said at the roundtable. But loosely prescribed standards and the range of risks involved made collating and analysing data expensive and difficult. Management functions often struggled to compile reliable DMAs.

"My function had to strongly challenge management's materiality assessment because they had chosen topics based on where we had reliable data and not on where the most material risks might be," a CAE from a financial services business in Italy said. In addition, because the external auditors did not have a complete view of the organisation's risk landscape, she also had to challenge their assessment.

"Internal auditors need to ask whether the double materiality assessment was completed properly in the first place," a CAE at a global automative company said. "Only then determine that the risks identified in the DMA are the correct material topics for your organisation." In organisations with gaps in their data, or that have immature reporting processes for CSRD, internal audit should focus on those control processes that are likely to cover a wide range of DMA topics. That information should be reported to management and the board with recommendations for improving both the quality and scope of controls, according to guidance by IIA Spain.

Circularity in the supply chain

Companies are increasingly strengthening circularity in their supply chains to reduce their dependency on the unpredictable supply of core materials in light of growing geopolitical pressures. In an interview for this report, one CAE of a global manufacturing company said that 20% of the business' revenue was now circular. Instead of simply focusing on mitigating ESG risks, organisations could consider circularity as a core strategy of adaptation to environmental change.



CLIMATE CHANGE, BIODIVERSITY AND ENVIRONMENTAL SUSTAINABILITY

Other CAEs agreed circularity was a key business driver in their sectors to help improve cost predictability and customer loyalty. Because of the rising costs of raw materials, especially from extractive industries, there was a growing case for embedding recycled products into supply chains, a CAE at a construction company in Austria said. As well as making commercial sense, he said that it had helped the business build a meaningful ESG story for stakeholders – although he warned that the internal audit function meticulously checked the data that was reported to minimise the risk of greenwashing. Internal audit also had a role to play in both informing the board on recent developments in the area and assessing their organisation's current levels of circularity.

"Internal auditors need to ask whether the double materiality assessment was completed properly in the first place."

How internal auditors can help organisations

1. Keep the board up to date with relevant changes to the regulatory environment
2. Provide assurance that quality data exists around the organisation's ESG risks to aid board decision-making and the reliability of reporting
3. Provide assurance that the organisation's business model takes adequate account of its long-term sustainability
4. Assess the double materiality assessment process to ensure that the full range of organisational risks is included from both perspectives
5. Provide challenge to management and external agencies (such as external auditors) about the assumptions and data used in double materiality assessments
6. Assess how far the organisation has considered the business case for supply chain circularity and where processes exist to identify gaps and opportunities
7. Keep the board up to date with recent developments in supply chain circularity to aid strategic decision-making

ABOUT RISK IN FOCUS

For the past 10 years, Risk in Focus has sought to highlight key risk areas to help internal auditors prepare their independent risk assessment work, annual planning and audit scoping. It helps Chief Audit Executives (CAEs) to understand how their peers view today's risk landscape as they prepare their forthcoming audit plans for the year ahead.

This year, Risk in Focus 2026 involved a collaboration between 14 European Institutes of Internal Auditors, spanning 15 countries including Austria, Belgium, France, Germany, Greece, Hungary, Ireland, Italy, Luxembourg, The Netherlands, Norway, Spain, Sweden, Switzerland and the UK.

The survey elicited 879 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

Institute of Internal Auditors Belgium

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