Chartered Institute of Internal Auditors

Parliamentary briefing

Risk in Focus – The Top Business Risks in 2026

Date: January 2026

What is Risk in Focus?

Risk in Focus 2026 is the Chartered Institute of Internal Auditors' annual flagship research project. It examines the most significant risks facing organisations across the UK and Europe and sets out how Chief Internal Auditors expect these risks to develop in 2026 and the years ahead.

For parliamentarians, the findings offer valuable insight into the pressures shaping business resilience, economic performance and organisational governance, as well as the vital role internal audit plays in providing independent assurance over these risks.

This year's project brings together the perspectives of 14 European Institutes of Internal Auditors across 15 countries, including Austria, Belgium, France, Germany, Greece, Hungary, Ireland, Italy, Luxembourg, the Netherlands, Norway, Spain, Sweden, Switzerland and the UK.

The research draws on a survey of nearly 900 Chief Internal Auditors, supported by one-to-one interviews with Chief Internal Auditors, Audit Committee Chairs and industry experts. These insights were complemented by five roundtable events, offering a richer understanding of the risk landscape organisations are navigating. You can read the full report here.

Risk in Focus 2026: Cybersecurity Dominates the Top Spot

Risk in Focus 2026 highlights the continued dominance of cybersecurity as the top risk for organisations, following a wave of high-profile attacks on M&S, the Co-Op, Harrods, The North Face and Jaguar Land Rover. These incidents reflect the growing severity of cyber threats and the heightened warnings from the National Cyber Security Centre about persistent risks from hostile states.

The report also shows digital disruption, new technology, and AI rising sharply as strategic risks, driven by rapid advances in generative AI. Talent management remains a major challenge, with shortages in digital and analytical skills and growing fears of AI-driven deskilling. Macroeconomic and geopolitical uncertainty also features prominently, with an unpredictable tariff war and global instability influencing almost every other risk category

Key Risks Identified in Risk in Focus 2026

Cybersecurity and Data Security

Cybersecurity remains the biggest risk for organisations going into 2026, with 82% of Chief Internal Auditors identifying it as their most significant threat and 62% ranking it as their organisation's first or second priority. High-profile incidents involving M&S, the Co-Op, Harrods, The North Face and Jaguar Land Rover illustrate why this risk continues to dominate. The ransomware attack on M&S alone is estimated to have cost the business £300 million, while an independent analysis by the Cyber Monitoring Centre estimates that the Jaguar Land Rover breach could cost the UK economy around £1.9 billion, making it the most financially damaging cyberattack in UK history. This attack disrupted thousands of suppliers and jobs, underlining the wider economic impacts of major cyber incidents.

Chief Internal Auditors reported a rise in AI-generated phishing attempts, deepfake attacks targeting senior personnel and successful breaches of multi-factor authentication systems, once seen as a gold-standard control. Many of these threats are believed to be linked to hostile state-sponsored actors such as China and Russia, increasing concerns about how the growing digitalisation of organisations amplifies the potential impact of a breach.

For parliamentarians, these developments carry clear national security implications. Cyberattacks increasingly target critical infrastructure, sensitive data and essential public services. They intersect with wider geopolitical tensions and highlight the importance of ensuring that UK organisations have the governance, skills and resilience needed to respond to fast-evolving digital threats.

Internal audit plays a central role in strengthening organisations' cyber resilience. Our research shows that cybersecurity is now where internal audit teams spend the most time, reflecting how serious and fast-moving this threat has become. Internal audit provides independent assurance that organisations are identifying new and emerging risks and that key controls, such as multi-factor authentication, continue to operate effectively. It also checks whether third-party suppliers and contractors have robust cyber measures in place, recognising that a single vulnerability in the supply chain can rapidly create wider disruption.

Internal audit also reviews whether organisations have strong backup and recovery arrangements that would allow essential services to be restored quickly after an attack. It ensures that cyber governance takes account of geopolitical tensions and increasingly complex digital operations. By advising boards on longer-term technology risks and preparedness, internal audit helps organisations stay ahead of attackers, protect sensitive data and strengthen their overall resilience.

Digital disruption, new technology and AI

The rapid acceleration of generative AI in particular is creating significant uncertainty for organisations, with many Chief Internal Auditors reporting that the pace of innovation makes it difficult for boards and senior management to plan more than a few quarters ahead. Alongside generative AI, other emerging technologies such as quantum computing are developing quickly, increasing the pressure on organisations to monitor technological change while managing the risks it brings.

This year's findings show that organisations are adopting AI faster than they can put the necessary controls in place. Many are concerned about the risk of errors or sensitive information being exposed when AI tools are used without clear oversight. As AI begins to influence decisions that affect customers, employees and business operations, organisations also need confidence that they can explain and stand behind those decisions. Ensuring transparency and accountability in the use of AI is becoming increasingly important to protect trust and uphold good governance.

For parliamentarians, these developments carry clear economic and regulatory implications. Rapid AI investment across Europe, including the European Commission's €200 billion InvestAI initiative, is reshaping the competitive landscape. With the UK aiming to establish itself as a global AI leader, ensuring that regulation and standards keep pace with technological change will be essential so that organisations can innovate quickly while maintaining strong controls and public trust.

Internal audit plays an essential role in helping organisations navigate these fast-moving changes. Chief Internal Auditors report increasing demand from boards for independent insight and assurance on AI governance, third-party management and horizon scanning for emerging technologies. Internal audit can assess whether AI strategies are flexible enough to adapt to rapid developments, provide independent assurance over the effectiveness and transparency of AI governance, and evaluate controls around procurement, data security and AI literacy.

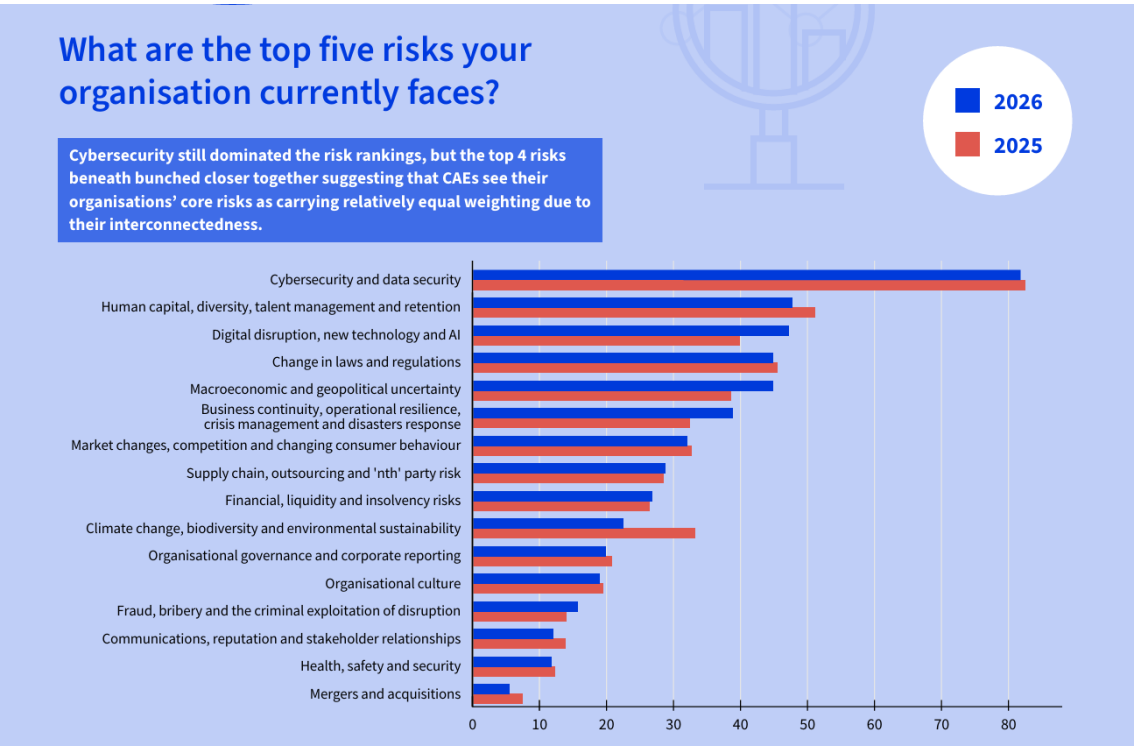
Macroeconomic and geopolitical uncertainty

Macroeconomic and geopolitical uncertainty remains a significant concern in 2026. Nearly a third of Chief Internal Auditors who selected this category said it was their organisation's top priority. They also stressed that this uncertainty cuts across other risk areas, reflecting a complex environment shaped by global trade disputes, volatile tariff decisions and ongoing global conflicts. Citigroup has described the impact of recent US tariff policies as Europe's "third once-in-a-lifetime shock" in fewer than five years, illustrating the severity of macroeconomic and geopolitical uncertainty currently.

These developments affect supply chains, business investment and energy prices, all of which weaken organisational resilience and contribute to subdued economic growth. With the World Bank expecting the global economy to reach its weakest levels since 2008, many organisations must balance rising external pressures with constrained budgets.

For parliamentarians, this instability affects economic resilience, business confidence and the UK's ability to compete in global markets. Sudden shifts in tariffs or political conditions can increase costs for consumers and create significant challenges for sectors that rely on stable international trade.

Internal audit helps organisations manage this instability by reviewing scenario planning, stress testing and governance processes. This assurance supports boards as they respond to sudden changes in geopolitical and economic conditions, strengthening organisational resilience in a volatile global environment.



Other key findings from Risk in Focus 2026:

• *Human capital, diversity, talent management and retention* – This remained the second-highest risk for 2026, with 48% of Chief Internal Auditors identifying it as a top concern. Persistent skills shortages, high staff turnover, and uncertainty about how AI will reshape careers and skills needs continue to put pressure on organisations.

• *Changes in laws and regulations* – This risk ranked joint 4th in 2026, reflecting the impact of shifting global policies, including uncertainty created by US tariff decisions and diverging regulatory approaches across Europe. Chief Internal Auditors highlighted concerns about the pace of regulatory change and the growing complexity of compliance requirements.

Contact us

We hope you find this briefing useful in understanding the key risks facing businesses in 2026. Should you have any further questions or require more information, please contact Gavin Hayes, Head of Policy and Public Affairs, at gavin.hayes@charterediia.org.