Chartered Institute of Internal Auditors

Parliamentary Briefing: Risk in Focus – The Top Business Risks in 2025

Issued: Tuesday 29 October 2024

What is Risk in Focus?

Risk in Focus 2025 is the Chartered Institute of Internal Auditors' annual flagship research project. The report analyses the top risks facing organisations across Europe and provides expert analysis on what Chief Internal Auditors perceive as their organisation's risk priorities for 2025 and beyond.

As a parliamentarian, it may be helpful for you to understand the top risks that businesses face and how internal audit plays a key role in helping to identify, manage, and mitigate these risks.

The project is 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 research is based on a survey of 985 Chief Internal Auditors, alongside one-to-one interviews with CAEs, Audit Committee Chairs, and industry experts. These interviews, combined with insights from five roundtable events, provided a deeper understanding of the key risks facing organisations. You can read the full report here.

Risk in Focus 2025

Risk in Focus 2025 reveals the ongoing dominance of **cybersecurity** as the number one risk for businesses, with increasingly sophisticated attacks posing serious challenges across sectors. AI-powered threats, alongside deepfake technologies, continue to transform the cyber landscape, requiring organisations to strengthen their defences. The report also highlights the rise of **digital disruption and AI** as significant risks, along with continued challenges in talent management and regulatory compliance.

KEY RISKS IDENTIFIED IN RISK IN FOCUS 2025

Cybersecurity and Data Security

Cybersecurity remains the top risk for businesses for 2025, **with 83% of Chief Internal Auditors identifying it as a major concern.** Organisations are facing increasingly sophisticated cyberattacks, including AI-driven threats like deepfake impersonations including those used to try and influence recent elections, making the protection of data and systems a matter of national importance.

Recent incidents, such as the TfL cyberattack and the NHS cyberattack, highlight the critical nature of this issue. These incidents caused major disruption to people's everyday lives, including disrupting transport services and threatening patient safety. This exposed serious vulnerabilities, demonstrating how cyber threats can impact both businesses and essential public services. Such incidents show how cyberattacks threaten critical infrastructure, erode public trust, and expose weaknesses in the UK's digital systems.

Given the rising complexity of these risks, parliamentarians must consider cybersecurity's role in safeguarding infrastructure and maintaining public confidence. Attacks on national institutions or services not only disrupt business operations but also undermine governance by compromising the integrity of government systems and exposing the sensitive personal and financial data of your constituents. As a result, cybersecurity is both a business priority and a matter of national security.

The Chartered IIA supports the introduction of the **Cyber Security and Resilience Bill**, along with the development of the **Cyber Governance Code of Practice**, which will help businesses assess and improve their cyber-risk management and governance practices. Internal audit plays a crucial role by independently assessing the effectiveness of cybersecurity controls and risk management. This includes evaluating the robustness of cyber governance and ensuring that organisations are prepared for emerging threats.

Internal audit teams can conduct independent penetration testing and can also engage ethical hackers to simulate attacks, identifying vulnerabilities and weaknesses in the system. By providing these independent assessments, internal audit ensures that cybersecurity measures remain strong, adaptable, and responsive to new challenges. This proactive approach supports both public and private organisations in maintaining business continuity and safeguarding public trust in the face of growing cyber threats.

AI and Digital Disruption: The Fastest Rising Risk

Artificial intelligence (AI) and digital disruption are transforming the business landscape at an unprecedented pace. Ranked as the fastest-growing risk for 2025, **40% of Chief Internal Auditors now place AI and digital disruption among their top five risks, up from a third (33%) a year ago**. This reflects the urgency with which businesses are grappling with the rapid integration of AI into their operations.

AI presents enormous opportunities, from increasing operational efficiency to revolutionising customer services. However, it also brings significant challenges. Issues around data privacy, the ethical use of AI, and the risk of automation-driven job displacement are becoming key concerns. Parliamentarians in particular will appreciate the legislative and ethical dimensions of AI, as the balance between innovation and regulation will be central to driving economic growth while ensuring appropriate safeguards are in place.

The Risk in Focus 2025 report highlights that by 2028, AI is expected to be the second biggest risk for businesses. This will necessitate a shift in how organisations audit their use of AI, ensuring that the technology is governed responsibly and that associated risks are managed effectively. The role of internal audit will be important when monitoring AI implementation, providing assurance on ethical AI use, and helping businesses remain compliant with evolving regulations.

Macroeconomic and Geopolitical Uncertainty

Macroeconomic and geopolitical uncertainty continues to be a major concern for 2025**, with 39% of Chief Internal Auditors ranking it among their top five risks.** Ongoing global conflicts, such as the war in Ukraine and the conflict in the Middle East, are disrupting supply chains, trade, and business operations. Additionally, state-sponsored cyberattacks and "grey zone aggression" — actions by state and non-state actors aimed at destabilising economies — are becoming more frequent.

For parliamentarians, this macroeconomic uncertainty directly impacts business performance, which in turn affects economic growth and national resilience. Disruptions to supply chains and key industries can lead to reduced productivity, job losses, and weaker economic performance. Geopolitical instability can also increase costs for businesses, particularly in areas such as energy and essential goods, which can affect the broader economy.

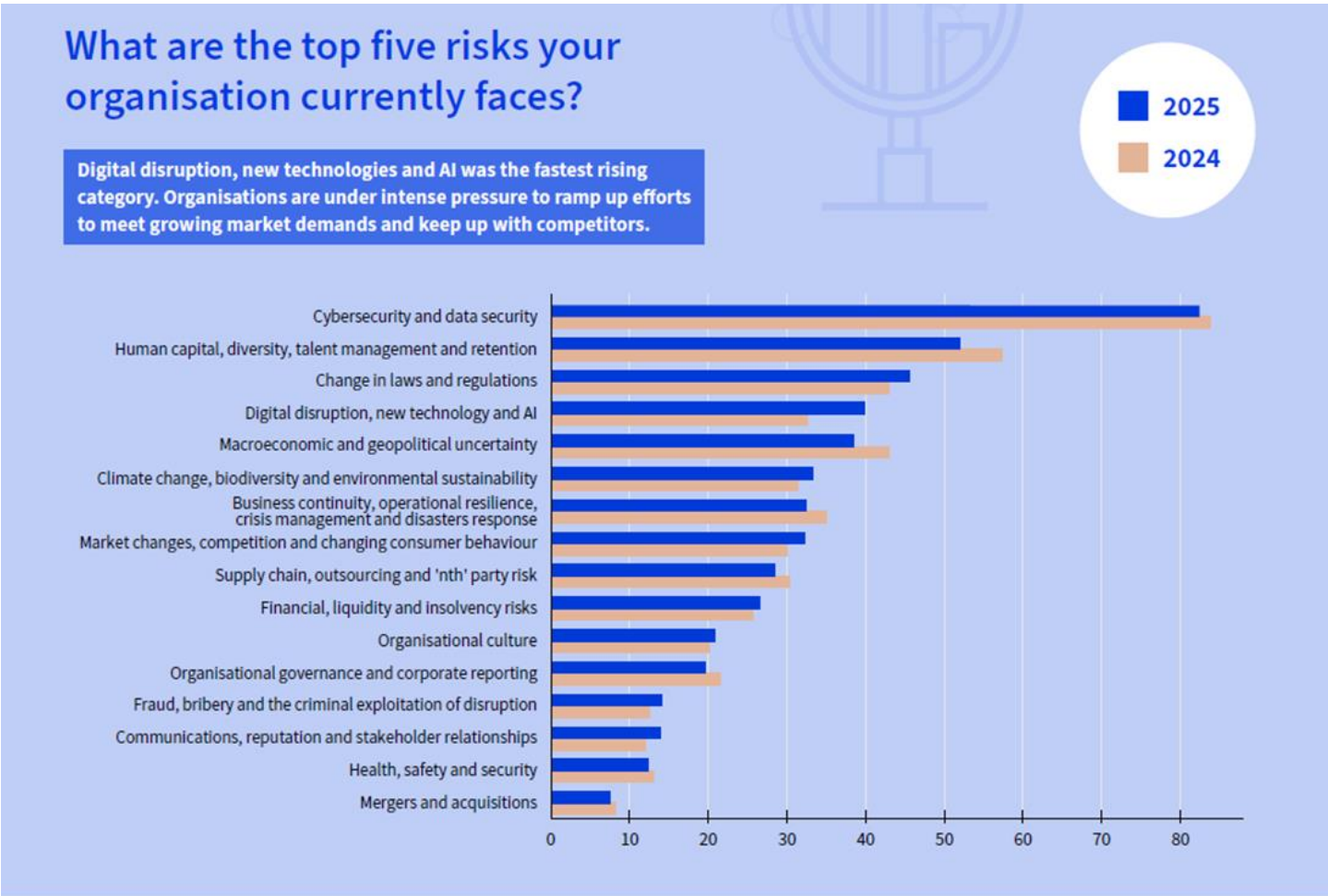
Internal audit can play a role in helping organisations navigate these risks. By reviewing scenario planning and stress-testing processes, internal audit can be a catalyst for improvement that helps the business ensure that they are resilient and able to adapt to sudden changes in the geopolitical environment. This resilience not only helps businesses maintain continuity but also supports the overall stability of the economy.

Climate Change, Biodiversity, and Environmental Sustainability

33% of Chief Internal Auditors highlighted climate change, biodiversity, and environmental sustainability as top risks for 2025. With increasing instances of extreme weather events and growing pressure to adopt sustainable practices, organisations are becoming more aware of the challenges posed by climate-related risks.

Parliamentarians need to be aware that businesses face greater exposure to both environmental impacts and regulatory changes. Compliance with new legislation, such as the EU's Corporate Sustainability Reporting Directive (CSRD), will require businesses operating in the EU to enhance their transparency around climate-related risks and sustainability efforts. Failure to adapt to these requirements not only risks regulatory penalties but could also impact business continuity and economic growth.

Internal audit can help organisations assess and manage their sustainability strategies. By providing assurance over compliance with evolving regulations and integrating climate risks into broader business strategies, internal audit supports the resilience of businesses in the face of increasing environmental pressures.



Other key findings from Risk in Focus 2025:

- **Changes in laws and regulations** – **With 46% of respondents identifying this as a top risk,** businesses are increasingly concerned about navigating a complex regulatory landscape, including new data protection, environmental sustainability, and corporate governance laws.
- **Human capital, diversity, talent management, and retention** – **This risk held its second-place ranking, with over half (52%)** of Chief Internal Auditors placing it as a top five concern. Balancing shifting demographic trends with skills and budgetary shortages during a time of increased digitalisation remains a key challenge for many organisations.

Chartered Institute of Internal Auditors

The Chartered Institute of Internal Auditors is the only professional body dedicated exclusively to championing and supporting the vital work of internal audit professionals in the UK and Ireland. It provides its more than 10,000 members with exceptional learning opportunities and is the only internal audit organisation in the world with a Royal Charter and therefore the authority to award chartered status.

Contact us

We hope you find this briefing useful in understanding the key risks facing businesses in 2025. Should you have any further questions or require more information, contact **Gavin Hayes, Head of Policy and Public Affairs, at gavin.hayes@iia.org.uk.**