# UK to expand AI oversight with new cyber resilience law



The UK Government is preparing to introduce the Cyber Security and Resilience Bill, a major legislative move that signals a growing global shift towards tighter regulation of artificial intelligence. The bill aims to strengthen oversight of digital services and supply chains, equipping regulators with new enforcement powers and mandating the timely reporting of significant cyber incidents.

This comes as governments and regulators worldwide grapple with the complex task of managing AI risks while fostering innovation. In Europe, new laws such as the Digital Operational Resilience Act (DORA) and Germany’s Supply Chain Act are reshaping how organisations approach risk, compliance and accountability.

The UK’s bill, expected later this year, expands the scope of cyber regulation beyond traditional IT systems. Regulators will be empowered to issue binding instructions and intervene when national security is at stake. A central provision requires companies to report major cyber breaches within defined timeframes—an urgent step following high-profile incidents such as the cyber attack on the NHS, which exposed vulnerabilities among critical service providers.

Across the EU, DORA is tightening ICT risk standards in the financial sector with rules on incident reporting, resilience testing and oversight of third-party providers. Germany’s Supply Chain Act adds another layer by requiring companies to uphold human rights and environmental standards across their global operations, backed by legal accountability for non-compliance.

As AI becomes increasingly embedded in business operations, regulators are expanding their focus beyond AI-specific tools to include intersecting risks such as data privacy, corruption and supply chain exposure. For companies, this demands a strategic shift—embedding compliance into innovation processes and adopting a proactive, integrated governance approach.

This includes addressing key questions: Are AI systems protecting user data and ensuring privacy? Are safeguards in place to counter algorithmic bias? Can AI decisions be explained transparently? Do compliance measures extend to third parties and global operations? Tackling these questions head-on enables organisations to build adaptable frameworks that align ethics with regulation.

Cross-functional collaboration is essential. Effective AI governance involves legal, compliance, IT and product teams working together to anticipate and mitigate risks. Establishing internal ethics boards, sharing knowledge across departments and consulting external experts all contribute to responsive and responsible oversight.

Transparency and ethical practices are increasingly seen as strategic advantages. Frequent audits, open communication and clear documentation of risks and safeguards reassure stakeholders, reduce reputational risk and build customer trust.

Continuous learning also plays a critical role. Role-specific training informed by skills assessments ensures employees are equipped to manage AI responsibly. A culture of ongoing education prepares organisations to evolve alongside rapid technological and regulatory change.

Ultimately, those best positioned to lead in AI will combine agile governance, cross-department collaboration, transparency and workforce development. The UK’s upcoming legislation, alongside complementary regulations in the EU and Germany, underscores the need to integrate accountability and resilience into AI strategies from the outset.

Embracing these changes will not only ensure compliance but also enable businesses to build trust and innovate responsibly—securing the UK’s position at the forefront of global AI leadership.

Created by [Amplify](https://www.hbmadvisory.com/amplify): AI-augmented, human-curated content.

## Bibliography

1. <https://www.techzine.eu/experts/privacy-compliance/132404/how-organisations-can-remain-compliant-while-building-resiliency-during-the-ai-era/> - Please view link - unable to able to access data
2. <https://www.gov.uk/government/collections/cyber-security-and-resilience-bill> - The UK government's Cyber Security and Resilience Bill aims to bolster the nation's cyber defences by expanding the scope of existing regulations to include more digital services and supply chains. It seeks to empower regulators with enhanced oversight and enforcement capabilities, including the ability to issue binding instructions to organisations and to intervene directly in cases of significant national security threats. The Bill also introduces mandatory incident reporting requirements, mandating organisations to report significant cyber incidents within specified timeframes. These measures are designed to strengthen the UK's resilience against cyber threats and protect critical infrastructure.
3. <https://www.eiopa.europa.eu/what-we-do/initiatives-and-activities/digital-operational-resilience-act_en> - The Digital Operational Resilience Act (DORA) is a European Union regulation aimed at enhancing the digital operational resilience of the financial sector. It establishes a comprehensive framework for managing information and communication technology (ICT) risks, ensuring that financial entities can withstand, respond to, and recover from ICT-related disruptions. DORA sets out requirements for ICT risk management, incident reporting, digital operational resilience testing, and oversight of critical ICT third-party service providers, thereby strengthening the EU's financial system against cyber threats and operational disruptions.
4. <https://www.csr-in-deutschland.de/en/gesetz-ueber-sorgfaltspflichten-in-der-supply-chain/> - Germany's Supply Chain Act, officially known as the Act on Corporate Due Diligence in Supply Chains, requires large companies to ensure that human rights and environmental standards are upheld throughout their supply chains. The law mandates companies to establish risk management systems, conduct regular risk analyses, and implement preventive measures to address identified risks. It also includes reporting obligations and provides for civil liability in cases of non-compliance, aiming to promote responsible business practices and protect human rights and the environment within global supply chains.
5. <https://www.ft.com/content/2388ff54-2fae-4893-87df-fd3c259bfcf6> - In response to a significant cyber attack on the UK's NHS by a Russian group, which caused major disruptions for thousands of patients, the UK government plans to implement stricter cyber security measures for private providers of essential public services. Unveiled in the King's Speech, the proposed Cyber Security and Resilience Bill aims to address the vulnerabilities of digital supply chains serving state institutions. The legislation will enhance cyber security rules and reporting requirements, aiming to make UK infrastructure and economy less vulnerable compared to the EU. The bill also seeks to empower regulators to investigate and enforce cyber security standards, particularly in healthcare, which is a major target for cyber attacks. Experts stress the need for effective implementation and enforcement to prevent future disruptions and protect patient care.
6. <https://www.reuters.com/world/uk/kings-speech-guide-new-uk-governments-proposed-laws-2024-07-17/> - Britain's new Labour government, led by Prime Minister Keir Starmer, has unveiled its first set of proposed laws focused on rebuilding the country. Key policy plans include a Planning and Infrastructure Bill to increase home construction, an Employment Rights Bill to ban zero-hour contracts and enforce fairer working conditions, and a Budget Responsibility Bill to ensure any significant tax changes undergo an independent forecast. Other proposals include new tough measures on illegal migration, housing reforms to challenge unfair rent increases, financial regulations to aid smaller pension schemes, and substantial plans for climate and energy investments through GB Energy. Railways will return to government control once private contracts expire, and constitutional reforms aim to reduce hereditary peer rights in the House of Lords. A Crime and Policing Bill targets issues like shoplifting, while the Cyber Security and Resilience Bill will enhance incident reporting and cyber attack data collection. Further devolution powers will be granted to local leaders, and conversion therapy is set to be banned. The government also plans to phase out cigarette sales gradually for those born after 2009 and end tax breaks for private schools to support government-run schools.
7. <https://www.gov.uk/government/news/new-cyber-laws-to-safeguard-uk-economy-secure-long-term-growth> - The UK government has announced new cyber laws aimed at safeguarding the economy and ensuring long-term growth. The Cyber Security and Resilience Bill, set to be introduced later this year, will bolster the UK's online defences, protect the public, and safeguard growth. The Bill includes measures to boost protection of supply chains and critical national services, including IT service providers and suppliers. It reflects the government's commitment to addressing the growing range of online threats and enhancing the nation's cyber resilience.