# UK firms urged to treat AI compliance as catalyst for trust and innovation



As the UK seeks global leadership in artificial intelligence, navigating new regulatory frameworks is becoming mission-critical for organisations. The EU AI Act and the Digital Operational Resilience Act (DORA) are setting new benchmarks for ethical use, transparency and operational resilience—raising the bar for data governance across sectors.

The EU AI Act focuses on the ethical deployment of AI systems, mandating clear rules around transparency and accountability. DORA, targeting financial services but with broader implications, demands stronger digital resilience in the face of ICT risks. Both frameworks underline the need for organisations to embed governance structures capable of meeting both regulatory scrutiny and real-world performance demands.

To support this transition, experts have developed a seven-step framework to help leaders build robust, trusted data systems. Key actions include improving data quality and traceability, strengthening privacy protocols and developing clear AI governance strategies rooted in ethics and accountability.

For those directly affected by DORA, especially in finance and fintech, preparation involves implementing ICT risk frameworks, regular testing for digital resilience and clear incident reporting protocols. Organisations must also manage third-party risk, foster governance cultures and provide staff with the training needed to make compliance a daily norm rather than a one-off exercise.

Importantly, compliance is not just a regulatory hurdle—it is an opportunity to strengthen organisational trust. Transparent data practices and standardised third-party agreements can help mitigate risk and position businesses as responsible innovators. Security infrastructure must be robust and flexible, ready to evolve with emerging threats and shifting technological landscapes.

With 2025 compliance deadlines approaching, data leaders are being urged to act now. This includes dedicating sufficient resources, maintaining updated cybersecurity protocols and actively engaging with regulatory authorities. A forward-looking compliance strategy that emphasises ethical responsibility and resilience will place UK businesses in a strong position to lead globally.

While the regulatory environment may appear daunting, structured, strategic preparation offers a clear path forward. By embracing compliance as a foundation for innovation and trust, the UK’s AI sector can achieve its ambition to lead responsibly in the next chapter of digital transformation.

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

## Bibliography

1. <https://www.dbta.com/DBTA-Downloads/WhitePapers/7-steps-to-prepare-for-emerging-data-and-AI-regulations-14257.aspx> - Please view link - unable to able to access data
2. <https://www.dbta.com/DBTA-Downloads/WhitePapers/7-steps-to-prepare-for-emerging-data-and-AI-regulations-14257.aspx> - This white paper outlines seven strategic steps for organisations to build trusted, transparent, and compliant data practices in response to emerging data and AI regulations, such as the EU AI Act and the Digital Operational Resilience Act (DORA). The steps include understanding evolving regulations, enhancing data quality, lineage, and privacy, and mastering AI governance for transparency, ethics, and accountability. The report aims to help data leaders and Chief Data Officers (CDOs) stay ahead, secure their data, and lead with integrity.
3. <https://www.securitypalhq.com/blog/digital-operational-resilience-act-dora-6-steps-to-prepare-for-2024-25> - This article provides six manageable steps to help organisations prepare for the Digital Operational Resilience Act (DORA). The steps include establishing an ICT risk management framework, setting up incident reporting processes, regularly testing ICT systems, managing third-party risks, and establishing a clear governance structure. Each step is broken down into actionable tasks to ensure organisations are fully equipped to meet DORA's requirements and enhance their operational resilience.
4. <https://www.jdsupra.com/legalnews/preparing-for-the-digital-operational-2716829/> - This article discusses the Digital Operational Resilience Act (DORA), an EU regulation designed to bolster the resilience of financial entities against ICT risks. It outlines seven key actions for payments and fintech businesses to prepare for DORA, including conducting a comprehensive ICT risk assessment, establishing an ICT risk management framework, developing incident response plans, enhancing third-party risk management, preparing for threat-led penetration testing, establishing reporting and communication protocols, and providing training and awareness programs.
5. <https://www.cio.com/article/3836940/exploring-dora-9-steps-on-the-path-to-compliance.html> - This article explores nine steps organisations can take to comply with the Digital Operational Resilience Act (DORA). The steps include assessing whether the organisation falls under DORA's scope, conducting a comprehensive risk assessment, strengthening ICT security measures, developing an incident response plan, enabling resilience of critical functions, managing third-party risks, implementing governance and oversight, preparing for reporting and auditing, and fostering a culture of resilience.
6. <https://technative.io/how-companies-should-prepare-for-the-eu-ai-act-and-dora/> - This article discusses how companies should prepare for the EU AI Act and DORA. It emphasises the need for organisations to review and update their contractual relationships, establish clear instructions on handling sensitive data, ensure transparent reporting, and implement robust security measures. The article also highlights the importance of consistent staff training to ensure compliance with the new regulations.
7. <https://www.sans.org/blog/how-to-prepare-for-dora-before-the-2025-deadline/> - This blog post outlines how organisations can prepare for the Digital Operational Resilience Act (DORA) before the 2025 deadline. It discusses the implications of DORA for financial organisations, including the need for a comprehensive ICT risk management framework, third-party risk management, mandatory resilience testing, and incident reporting. The post provides strategies for effective DORA compliance, such as developing and updating cybersecurity policies, implementing robust security measures, establishing incident detection and management processes, conducting digital operational resilience testing, managing ICT third-party risk, implementing strong authentication mechanisms, training and educating staff, cooperating with supervisory authorities, allocating appropriate resources, and staying informed and agile.