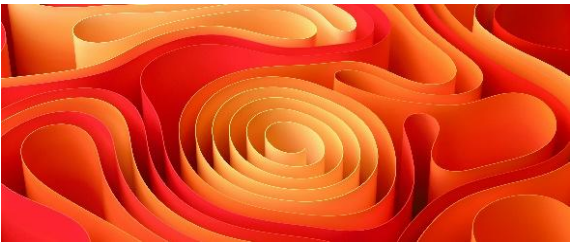
Pills

Regulatory/Supervisory Pills | N.84 June 2026

Author: Dario Esposito



TOPICS:

Model Risk

SOURCE:

Bank of England, Financial Conduct Authority & His Majesty's Treasury

BoE, FCA and HM Treasury Joint Statement on Frontier AI Models and Cyber Resilience

- The joint statement addresses the growing **cyber resilience risks associated with frontier artificial intelligence (AI) models** and outlines supervisory expectations for regulated financial firms. The statement emphasizes that frontier AI technologies represent a significant escalation in cyber capability, enabling **malicious actors to conduct attacks more rapidly, at greater scale and at lower cost** than previously possible.
- The document **reinforces existing operational resilience and cyber security expectations** rather than introducing new regulatory obligations. It highlights that firms and financial market infrastructures (FMIs) must proactively strengthen their cyber resilience frameworks to address AI-driven threats. Regulators stress the importance of effective preventive, detective, containment, response and recovery capabilities, particularly as frontier AI systems evolve further.
- A key focus of the statement is **governance and strategic oversight**. Boards and senior management are expected to develop sufficient understanding of frontier AI-related risks to ensure informed decision-making, adequate investment and appropriate oversight of control functions. Firms are encouraged to review resourcing decisions, legacy system exposures and insurance coverage in light of the emerging threat landscape.
- The statement also places significant emphasis on **vulnerability management and third-party risk oversight**. Regulators expect firms to improve their ability to identify, prioritise, assess and remediate vulnerabilities rapidly and at scale, potentially through automation and AI-enabled tools. Particular attention is given to risks arising from external suppliers, open-source software and integrated third-party services, requiring firms to maintain robust monitoring and remediation capabilities across supply chains.
- Finally, the authorities encourage firms **to adopt AI-enabled defensive measures, maintain strong access and network controls and ensure rapid recovery from disruptions**.