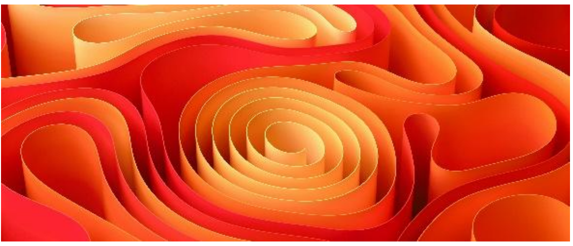
Pills

Regulatory/Supervisory Pills | N.112 July 2026

Author: Dario Esposito



TOPICS:

Cyber risk, AI Model

SOURCE:

European Systemic Risk Board, European Central Bank

ESRB-ECB: Frontier AI Models Could Strain Cyber Resilience in the Financial System

- The ESRB Warning and the accompanying ECB Supervisory Letter highlight the growing systemic **cyber risks** posed by **Frontier AI Models (FAIMs)** and call for an accelerated strengthening of the financial sector's cyber resilience. Together, the two documents underline that **existing regulatory frameworks remain appropriate but require faster implementation, stronger board oversight and greater preparedness** to address the rapidly evolving AI-driven cyber threat landscape.
- The **ESRB** warns that **FAIMs can autonomously identify software vulnerabilities, generate exploits and execute sophisticated cyber-attacks at unprecedented speed and scale**, significantly reducing the time available for financial institutions to detect, assess and remediate vulnerabilities. This "collapse of defensive time buffers" could overwhelm existing patch management processes and increase the risk of simultaneous cyber incidents with systemic implications.

  The ESRB identifies key vulnerabilities including reduced response times, increased reliance on a small number of AI and cloud providers, and the need for stronger supervisory preparedness and sector-wide coordination within the existing EU regulatory framework, notably **DORA**, the **AI Act** and the **Cyber Resilience Act**.
- The **ECB** translates these concerns into **supervisory expectations for significant institutions**. Banks are expected to promptly address existing cybersecurity weaknesses and submit, by **31 October 2026, a comprehensive action plan** outlining measures to strengthen vulnerability management, AI-enabled cyber defences, third-party risk management, governance and operational resilience.