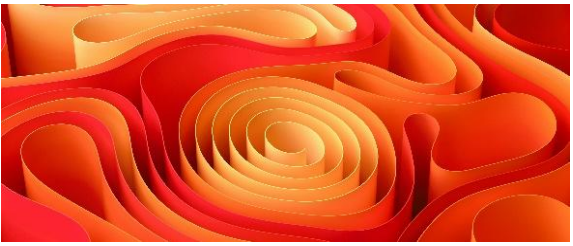
Pills

Regulatory/Supervisory Pills | N.132 September 2026

Author: Dario Esposito



TOPICS:

ICT risk

SOURCE:

European Supervisory Authorities

EBA, EIOPA and ESMA Call for Enhanced Governance and Consistent Supervision to Mitigate ICT Risks From Frontier AI

- This ESAs Statement provides **supervisory guidance** for financial entities **on managing** the increasing **cybersecurity risks posed by** highly capable **frontier AI models**. The statement is intended **to complement** - not replace - **the existing EU regulatory framework**, particularly the Digital Operational Resilience Act (DORA) and the AI Act.
- The ESAs highlight that frontier **AI models can significantly accelerate cyberattacks** by enabling rapid vulnerability discovery, automated exploitation and attacks on shared infrastructure or critical dependencies. While these technologies also strengthen defensive capabilities, their misuse could create systemic operational disruptions affecting multiple financial institutions and, potentially, the wider financial system.
- The statement emphasises that financial entities should proactively strengthen **ICT risk management using a risk-based and proportionate approach**, reflecting each entity's size, complexity, interconnectedness, and risk profile, in line with DORA. Supervisory authorities are expected to focus on governance, operational resilience, and timely remediation of identified ICT weaknesses.
- To address these risks, the ESAs organise recommended actions into **three** complementary **pillars**: 1) **Prevention** - Maintain comprehensive ICT asset inventories, adopt secure-by-design principles, minimise attack surfaces, automate vulnerability management and patching, strengthen identity and access management, protect source code and reinforce cybersecurity standards across supply chains; 2) **Detection** - Shift from periodic to continuous monitoring through real-time vulnerability scanning, enhanced logging and behavioural analytics, more frequent testing, and AI-supported security operations to improve the speed of threat detection and response; 3) **Risk management and operational resilience** - Update incident response and business continuity arrangements to address AI-assisted attacks, strengthen backup and disaster recovery capabilities, conduct resilience testing against AI-enabled threat scenarios, monitor ICT dependencies, enhance management accountability, automate risk escalation, and improve cybersecurity awareness across the organisation.