Just in Time

Systemic Cyber Risks from Frontier AI Models and Supervisory Expectations for Significant Institutions

September 2026

iason ESSENTIAL SERVICES FOR FINANCIAL INSTITUTIONS

Executive Summary

- The **ESRB** Warning identifies **Frontier Artificial Intelligence Models (FAIMs)** as an emerging source of **systemic risk** to the European financial system, arguing that these models fundamentally alter the balance between attackers and defenders and have the potential to undermine the operational resilience of the financial system as a whole.
- Building upon this assessment, the **ECB** "Dear CEO Letter" translates these concerns into concrete supervisory expectations for Significant Institutions (SIs), requiring them to assess without delay the implications of the evolving cyber threat landscape and to submit a comprehensive action plan by **31 October 2026**.
- The central message conveyed by both documents is that the principal challenge does not stem from the emergence of entirely new categories of cyber threats, but rather from the unprecedented acceleration in the **speed, scale and sophistication** of cyber-attacks enabled by frontier AI.

At a Glance

Keywords: Frontier AI Models, Cyber Risk, Operational Resilience, Systemic Risk

01

A New Cybersecurity Paradigm

A New Cybersecurity Paradigm

Just in Time

Both documents[1] reach the same fundamental conclusion: **Frontier AI Models** represent a **genuine paradigm shift** in cybersecurity.

Traditionally:

- **vulnerability discovery required highly specialised expertise;**
- **exploit development typically took days or weeks;**
- **financial institutions had sufficient time to analyse vulnerabilities, test remediation measures and deploy software patches.**

Frontier AI fundamentally changes this model.

These advanced models are increasingly capable of:

- **identifying previously unknown vulnerabilities;**
- **developing functional exploits;**
- **automating entire attack chains;**
- **operating at a speed and level of sophistication comparable to, or exceeding, that of leading human experts.**

As a consequence, the time available for defensive action is dramatically reduced.

The ESRB describes this phenomenon as the **collapse of defensive time buffers**, while the ECB highlights the compression of the interval between vulnerability discovery and operational exploitation.

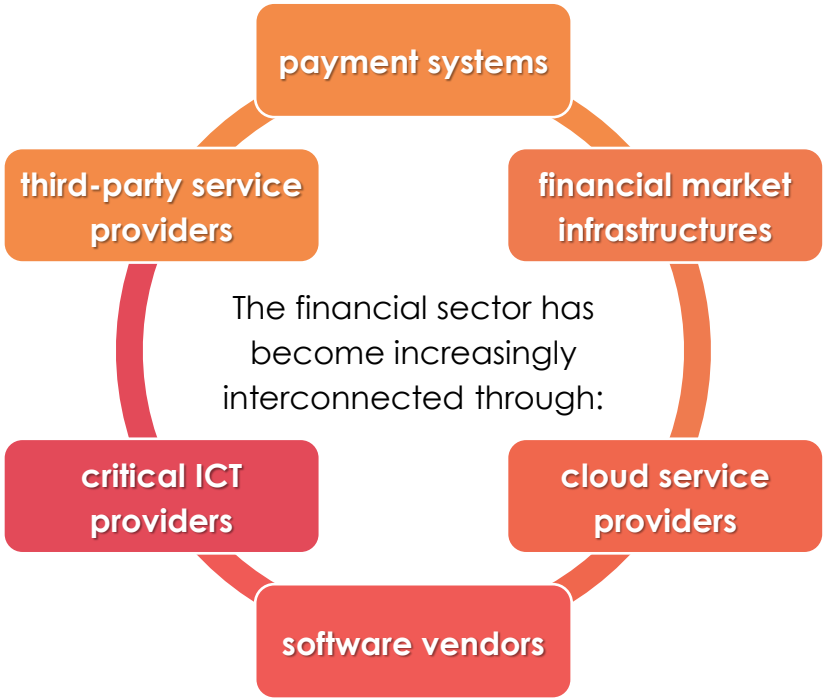
[1] The **ESRB** Warning and the **ECB** "Dear CEO Letter".

02

From Operational Risk to Systemic Risk

From Operational Risk to Systemic Risk

The ESRB's principal contribution is to **shift the focus from the resilience** of individual institutions to the **stability of the financial system** as a whole.



Within such an interconnected ecosystem, the simultaneous exploitation of multiple vulnerabilities could trigger:

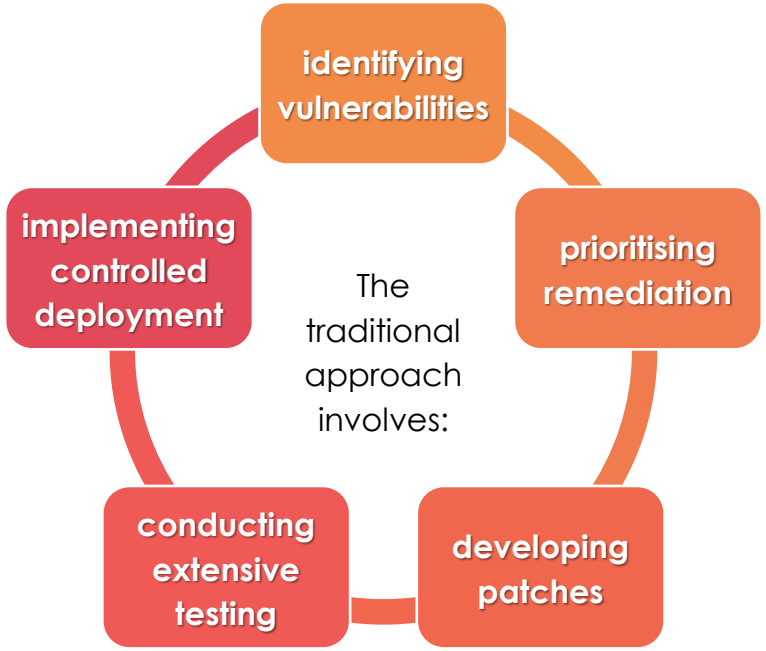
The ECB incorporates this analysis into its **supervisory expectations** by emphasizing that **vulnerabilities** already identified - but not yet remediated - may become significantly more **critical** in the new threat environment.
Accordingly, **banks are encouraged to address without delay all outstanding supervisory findings relating to ICT security**.

03

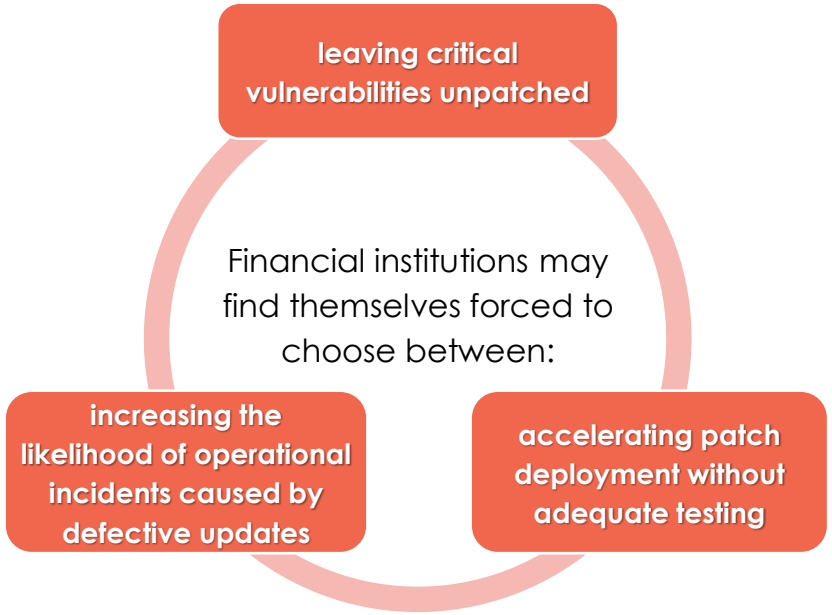
Why Existing Cybersecurity Practices May No Longer Be Sufficient

Why Existing Cybersecurity Practices May No Longer Be Sufficient

Both documents acknowledge that current vulnerability management processes were designed for a very different threat environment.



However, the exponential increase in ***vulnerabilities identified by frontier AI could overwhelm these processes.***



Consequently, the ECB explicitly calls upon institutions to **enhance vulnerability management** at scale by strengthening ICT resources, revising change management processes and preparing for substantially more frequent patch deployment.

04

The Three Structural Asymmetries Introduced by Frontier AI

The Three Structural Asymmetries Introduced by Frontier AI

Just in Time

One of the most significant analytical contributions of the ESRB Warning is the **identification of three structural asymmetries** created or amplified by **Frontier AI**.

Geopolitical Asymmetry

Most leading Frontier AI developers are currently located outside the European Union.

This creates:

- technological dependency;
- geopolitical exposure;
- unequal access to advanced defensive AI capabilities.

The ESRB therefore advocates timely and proportionate mechanisms to ensure adequate access to Frontier AI capabilities across all Member States, thereby preserving the integrity of the Single Market and avoiding fragmentation.

Attacker–Defender Asymmetry

Frontier AI dramatically lowers the barriers to entry for malicious actors.

Activities that previously required:

- years of specialist expertise;
- extensive technical knowledge;
- significant financial resources,

can increasingly be automated.

By contrast, defenders remain constrained by:

- regulatory obligations;
- governance requirements;
- operational continuity considerations;
- internal control frameworks.

The ECB therefore expects financial institutions to strengthen:

- continuous monitoring;
- threat detection;
- AI-assisted defensive capabilities.

Asymmetry Among Financial Institutions

Large institutions generally possess:

- greater financial resources;
- dedicated cybersecurity specialists;
- advanced technological capabilities;
- stronger governance frameworks.

Smaller institutions may lack equivalent resources.

Since systemic resilience ultimately depends upon the resilience of the weakest participants, disparities in preparedness themselves become a source of systemic risk.

05

Supervisory Expectations from the ECB

Supervisory Expectations from the ECB

Just in Time

The ECB Supervisory Letter effectively translates the ESRB's systemic assessment into operational supervisory expectations.

Each Significant Institution is expected to prepare a comprehensive **Action Plan** by **31 October 2026**, setting out both immediate and longer-term measures.

Immediate Priorities

Accelerating Vulnerability Management

Banks are expected to:

- increase the frequency of vulnerability scanning;
- leverage AI-enabled security tools where appropriate;
- accelerate patch management processes;
- adapt change management procedures to the evolving threat landscape.

Securing the Attack Surface

Particular attention should be paid to:

- internet-facing systems;
- cloud environments;
- VPN infrastructures;
- open-source software;
- third-party applications;
- emerging technologies.

Strengthening Detection Capabilities

The ECB encourages institutions to reinforce:

- continuous log monitoring;
- network traffic analysis;
- rapid identification of indicators of compromise;
- AI-supported threat detection capabilities.

Managing Third-Party Risk

The supervisory expectations extend beyond the institution itself.

Banks should ensure that external service providers are capable of:

- managing accelerated vulnerability disclosure;
- implementing rapid patch deployment;
- coordinating incident response effectively.

06

Governance and Strategic Investment

Governance and Strategic Investment

Just in Time

Both documents place considerable emphasis on **governance**.

Boards of Directors are expected to assess whether current:

1. ICT investment
2. staffing levels
3. financial resources
4. governance arrangements
5. risk appetite
6. change management capabilities

remain adequate in light of the evolving cyber threat landscape.

The **ECB** further expects each Action Plan to define:

1. clear ownership and accountability
2. implementation milestones
3. allocated resources
4. monitoring and reporting arrangements

07

Long-Term Structural Measures

Long-Term Structural Measures

Just in Time

Alongside immediate actions, the ECB identifies **several structural priorities** for strengthening **resilience** over the longer term.

These include:

1. **modernising legacy technology**
2. **decommissioning end-of-life systems**
3. **strengthening cyber hygiene**
4. **enhancing defence-in-depth architectures**
5. **improving incident response and recovery capabilities**
6. **reinforcing crisis management arrangements**
7. **promoting information sharing across the financial sector**

The ESRB notes that these developments should progressively be **incorporated** into **supervisory methodologies**, **macroprudential assessments** and **cyber resilience stress testing**.

08

Regulatory Framework

Regulatory Framework

Both documents make clear that the evolving threat landscape does not necessarily require entirely new **legislation**.

Instead, authorities emphasise the need for **a more coordinated and rigorous application of existing regulatory frameworks**, including:

- **Digital Operational Resilience Act (DORA)**
- **Artificial Intelligence Act**
- **Cyber Resilience Act**
- **NIS2 Directive**
- **EU Systemic Cyber Incident Coordination Framework (EU-SCICF)**

*The ECB also highlights **ongoing international cooperation through the G7**, the **Basel Committee on Banking Supervision** and the **Financial Stability Board**.*

09

Expectations in Short Term & Medium Term

Expectations in Short Term & Medium Term

Just in Time

Both publications characterise the current period as a **transitional phase**.

In the **short term**:	
1	offensive AI capabilities are expected to evolve more rapidly than defensive capabilities
2	operational cyber risk is likely to increase
3	pressure on ICT and cybersecurity functions will intensify

Over the **medium term**:	
1	financial institutions are expected to benefit increasingly from AI-enabled defensive capabilities
2	supervisory frameworks will continue to evolve
3	the ESRB will maintain continuous monitoring of AI-related systemic cyber risk through its regular macroprudential assessments

The ECB also signals that **future supervisory attention** will extend to **risks associated with quantum computing** and the **transition towards post-quantum cryptography**.

10

Conclusions & Take Aways

Conclusions & Take Aways

Just in Time

1. The ESRB identifies Frontier AI Models as a new source of systemic risk to European financial stability, while the ECB translates this assessment into concrete supervisory expectations for Significant Institutions.
2. The most significant transformation concerns the dramatic reduction in the time available between vulnerability discovery and operational exploitation.
3. Existing vulnerability management processes may prove inadequate in an environment characterised by the large-scale discovery of vulnerabilities enabled by Frontier AI.
4. Financial institutions are expected to strengthen governance, ICT investment, vulnerability management, monitoring capabilities and third-party risk management.
5. Boards of Directors are expected to play a central role in overseeing cyber resilience and ensuring adequate strategic investment.
6. The Action Plan requested by the ECB by 31 October 2026 constitutes the principal supervisory mechanism through which these expectations should be translated into concrete implementation measures.
7. DORA remains the cornerstone of the European regulatory framework for operational resilience, but its application must increasingly reflect the evolving risks introduced by Frontier AI Models.
8. Close cooperation between supervisory authorities, financial institutions, technology providers and operators of critical infrastructure is considered essential to mitigating a threat that is now recognised as systemic rather than purely operational.

ESSENTIAL SERVICES FOR FINANCIAL INSTITUTIONS

iason is an international consulting firm that has been supporting both financial institutions and regulators in topics related to Risk Management, Finance and ICT since 2008

Strategy

Strategic advisory on the **design** of **advanced frameworks** and **solutions** to fulfil both **business** and **regulatory needs** in Risk Management and IT departments

Methodology & Governance

Implementation of the designed **solutions** in bank departments **Methodological support** to both **systemically important financial institutions** and **supervisory entities**

Solution

Advanced **software solutions** for **modelling, forecasting, calculating** metrics and **integrating** risks, all on cloud and distributed in Software-as-a-Service (**SaaS**)

KEEP IN TOUCH

iason

Company Profile

iason is an international firm that consults Financial Institutions on Risk Management. **iason** integrates deep industry knowledge with specialised expertise in Market, Liquidity, Funding, Credit and Counterparty Risk, in Organisational Set-Up and in Strategic Planning.

Dario Esposito

Lorena Corna

www.iasonltd.com