JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

31 July 2026

JC 2026 25

# ESA Statement

# Toward a consistent and risk-based approach for ICT risks from frontier AI models

1. The advanced capabilities of recent frontier AI models significantly accelerate cyber risks, underscoring the urgent need for robust cybersecurity measures and rapid incident response capabilities. AI-enabled cyber tools could generate systemic risks due to their ability to: i) rapidly discover and exploit vulnerabilities; ii) target vulnerabilities in shared infrastructure; and iii) leverage single points of failure across entities[1]. While these models can help deliver substantial defensive improvements, they can also provide an advantage to malicious actors, which could leverage these capabilities, while defenders need to implement their responses following quality assured protocols.

2. On 7 July, the European Commission published its Action Plan on Cybersecurity and Artificial Intelligence to reinforce the EU's cybersecurity and resilience[2]. In this context, the ESRB stressed in its issues note and in its warning[3] that the misuse of highly capable AI models could have a substantial impact in the financial system. If such disruptions persist for several days or affect multiple institutions simultaneously, the consequences could extend beyond individual entities to the broader financial system and the real economy. Likewise, ENISA published an initial set of recommendations to develop the operational capabilities of the various stakeholders to face these risks[4].

3. Therefore, the supervisory dialogue with the financial entities pays particular attention to these risks and to the measures financial entities have in place to safeguard operational resilience. In particular, the ECB has emphasised to the CEOs of the significant institutions[5] the importance of addressing, without delay, open supervisory findings and measures related to the ICT areas in focus and security risks that have been identified in previous supervisory activities such as on-site inspections, targeted reviews and the 2024 cyber-resilience stress test. Given the accelerating threat landscape, existing weaknesses that remain unresolved may become increasingly material and pose significant risks to operational resilience. Likewise, other competent authorities may set their supervisory expectations accordingly.

[1] See also IMF Blogpost (07th May 2026) Financial Stability Risks Mount as Artificial Intelligence Fuels Cyberattacks

[2] EU Action Plan on Cybersecurity and Artificial Intelligence | Shaping Europe's digital future

[3] Warning of the European Systemic Risk Board of 25 June 2026 on systemic cyber risks stemming from frontier artificial intelligence models (ESRB/2026/3)

[4] https://www.enisa.europa.eu/publications/enisas-view-on-cybersecurity-in-the-frontier-ai-era

[5] Addressing AI-enabled cybersecurity threats

4. The ESAs have a mandate to promote coordination between competent authorities and to foster supervisory convergence. Given the significant ICT risks stemming from frontier AI models, the goal of this ESA statement is to provide context to the current situation considering the existing legislation and supervisory expectations, through possible mitigating actions that financial entities may implement to address these risks. In this regard, the present ESA Statement is consistent with the initiatives and communications issued by the European Systemic Risk Board (ESRB), the ENISA and the competent authorities, and with the objectives of the European Commission Action Plan.

5. The current EU regulatory framework, especially the Digital Operational Resilience Act (DORA) and the AI Act, provide a solid foundation to tackle risks stemming from the release of highly capable AI models. The requirements set out in DORA remain highly relevant, through the implementation of the ICT risk management framework, testing, incident and recovery management and ICT third party risk management. The AI Act provides a framework for '*General-purpose AI models with systemic risk*', where providers are subject to additional obligations, including transparency, the provision of relevant technical documentation and cybersecurity aspects. While the regulatory framework remains technology-neutral, the shorter vulnerability discovery and exploitation cycles, led the ESAs to encourage financial entities to act fast and proactively, make the necessary arrangements to enhance their cybersecurity capabilities and adapt them to the new context. It is expected that financial entities implement measures in a proportionate manner, considering their size and overall risk profile, and the nature, scale and complexity of their services, activities and operations.

6. Consequently, to strengthen the risk mitigation, to promote a coordinated supervisory approach and ensure a level playing field across the EU, the ESAs encourage financial entities, taking into account the expectations of their supervisory authorities, to adjust ICT risk management processes, procedures and controls according to the following three risk mitigation strategies: i) prevention; ii) detection; iii) management. The Annex provides examples of risk mitigation strategies and potential actions that can be summarised as:

    - **Prevention** relies on comprehensive and continuously updated inventories of all IT assets (including infrastructure, applications, data repositories, APIs, and AI/ML components), as this enables financial entities to classify assets based on criticality and exposure. Secure-by-design principles ensure that systems are architected with built-in safeguards, rather than relying solely on reactive controls. Strong monitoring and proactive patching processes are essential to maintaining resilience against evolving threats and reduce the window of exposure. Assessing the risk from dependencies among IT assets is essential for consistently prioritising preventive measures.

    - **Detection** scales up existing vulnerability discovery processes, in terms of timeliness and complexity, to match the existing threats. Despite preventive measures, the perimeter might still be breached by AI-assisted threat actors. Therefore, detective measures are essential to identify, analyse, and respond to intrusions before they escalate into significant incidents. Monitoring processes transition from periodic to continuous, to reduce detection and response times, and enhance visibility into unusual or malicious behaviour. Security operation

centre (SOC) and red teaming capabilities can be enhanced with AI solutions in addition to existing technical and staff capabilities.

. **Management of** cyber risk to improve operational resilience, through operational resilience testing, enhanced disaster recovery, data backup capabilities and increased cyber maturity. Risk management frameworks, testing methodologies, and governance structures need to adapt to address AI-assisted threats and potential multi-system failures. In parallel, management bodies must ensure that accountability keeps pace with emerging risks, while cybersecurity awareness must evolve toward a more proactive and adaptive mindset. The amendment of existing IT risk management frameworks would potentially trigger needed updates on the business and IT architecture, alongside changes to business continuity plans.

7. In this context, competent authorities should also ensure that financial entities' management body is fully committed to mitigate frontier AI models-driven cyber risks, with clear governance and accountability frameworks in place, timely response plans adequately prepared, and sufficient internal investments dedicated to strengthening cyber resilience. The Risk Appetite Framework should be reviewed to update and/or incorporate metrics, tolerance thresholds, and control measures consistent with the evolving risk profile stemming both from the internal use of such models and from indirect exposure to them.

8. In all cases and without delay, the financial entities should establish governance structures that support effective management of frontier AI related risk and closely monitor this risk. While ideally financial entities try and match the speed and sophistication of AI-assisted threat actors, a one-size-fits-all approach when implementing these risk mitigation strategies would not be proportionate and efficient. Instead, entities shall take into account their size and overall risk profile, and the nature, interconnectedness, scale and complexity of their services, activities and operations when designing their risk mitigation strategies *(DORA Art.4).*

9. The ESAs will keep working with competent authorities to maintain a proportionate, risk-based and forward-looking approach regarding emerging risks from advanced AI models with cyber capabilities. Such combined efforts will aim at ensuring that the financial sector is sufficiently resilient, consistently with the objectives of the DORA framework.

10. Furthermore, the ESAs as Lead Overseers initiated targeted engagement with relevant CTPPs to understand how they identify and manage the new challenges they face. It covered the identification and assessment of the risks, the mitigation measures they have implemented, and their adaptation to the opportunities associated with these new capabilities. The insights gained have informed the annual risk assessment cycle and the prioritisation of activities under the 2027 Oversight Plan. The ESAs as Lead Overseers have also begun embedding AI-related risks into its Oversight Examination Methodology and will continue to strengthen this work throughout 2027. In parallel, these threats are expected to be reflected in the scope of the oversight examinations and other oversight activities in 2027 to assess the preparedness and resilience of CTPPs in an increasingly AI-enabled threat environment.

## Annex – Examples of risk mitigation strategies and actions

Financial entities may consider these risk mitigation strategies and actions taking into account their size, complexity, interconnectedness and risk exposure. This Annex does not establish additional requirements, nor should be regarded as a comprehensive checklist. Instead, it is to be read as illustrative examples to be considered by financial entities, also in their dialogue with ICT third-party service providers.

| Strategy | Risk | Potential actions to consider |
|---|---|---|
| **Prevention** | | |
| **Implement automated security controls into development, deployment, and operational workflows** | Traditional static security models may not be able to respond timely to AI-enhanced attacks as they rely on predefined rules, signatures, and fixed patterns, while AI-driven threats are dynamic and adaptive. | As referred to in Article 10 of the RTS RMF, measures may range from basic automated vulnerability scanning and patch management to (AI-augmented) "DevSecOps" (Development, Security, and Operations) practices, across the ICT-System lifecycle. |
| **Implement security and resilience by design principles** | AI's ability to analyse and exploit architectural flaws (such as poorly secured APIs, excessive permissions, or monolithic system designs) further emphasizes the need to embed security and resilience into systems from the outset. | Implement basic secure design principles, threat modelling, for critical systems and network segmentation, evolving towards more advanced techniques like zero-trust architectures and AI-driven threat modelling. |
| **Protect confidentiality of source code** | Highly capable AI-models can analyse leaked or exposed source code to identify vulnerabilities, backdoors, or proprietary algorithms, or even attempt to reverse engineer protected code in search of known vulnerabilities. | Protect proprietary source code and critical configuration confidentiality to reduce the attack surface available for automated discovery, slow down reconnaissance, improve the effectiveness of deception operations and limit the ability to exploit application weaknesses quickly and systematically. |

| | | |
|---|---|---|
| **Reduce the attack surface** | A larger attack surface provides more entry points for cyberattacks, which highly capable AI models may rapidly scan and analyse to identify weak spots, misconfigurations, or unpatched vulnerabilities at scale. The broader and more complex the attack surface, the easier it is for AI-powered adversaries to find and prioritize exploitable targets quickly. | Eliminate unnecessary exposures, enforcing segmentation, and decommissioning legacy systems. This can be achieved by applying, as a minimum, basic hygiene measures (e.g., inventory management), and evolving into more advanced techniques like AI-driven attack surface management. |
| **Proactive and automated patches for high/risk systems across all environments** | AI-driven attacks operate at machine speed, enabling vulnerability detection and exploitation in a very short time span. Traditional patching processes relying on periodic and reactive approach may not be sufficient to ensure a timely reaction. | Following a risk-based approach investigate proactive and automated patch processes for high-risk systems and patches, and aim towards extending these processes to all environments, including disaster recovery (DR) and backup systems.<br>Consider newly introduced or enhanced risks and ensure sufficient mitigating controls, such as clear criteria for which patches and systems to include, sufficient (automated) testing, monitoring, the deployment schedule, redundancies, or robust fallback plans and rollback procedures. |
| **Ensure that access management minimises permissions and reduces the likeliness of unauthorised access** | AI-driven attacks can bypass controls based on traditional methods, such as static passwords or perimeter-based security, mimic legitimate behaviour, and exploit trust relationships faster than legacy defences can respond. | The risk toolkit includes strict access controls, continuous monitoring, and multi-factor authentication (MFA) to limit the impact of breaches; as the maturity of the control environment grows, foundational requirements like basic MFA and least-privilege access may evolve into advanced techniques like behavioural analytics and just-in-time (JIT) access. |
| **Assess, monitor, and enforce cybersecurity standards across the whole supply chain** | In a supply chain attack, an attacker may compromise an entity through an ICT third-party service provider; this can be further | Assess, monitor, and enforce cybersecurity standards across the whole supply chain, with more rigorous controls for greater exposure and more complex supply |

| | | |
|---|---|---|
| | exploited by sophisticated AI models, which can identify weak links in the supply chain and automate multi-stage attacks. | chains. This includes not only services providers and partners but also soft- and hardware providers and open-source communities. |
| **Detection** | | |
| **Apply continuous vulnerability scanning and monitoring** | Periodic vulnerability scanning may no longer be sufficient in the face of AI-driven attacks, which can uncover zero-day vulnerabilities and exploit them immediately. | Employ continuous scanning and monitoring to detect and remediate weaknesses before they are exploited. Align the frequency and depth of scanning with the financial entity's risk profile: from basic automated scans to AI-driven, real-time vulnerability management. |
| **Implement comprehensive logging and behavioural monitoring while avoiding data overload** | AI-assisted attackers can generate unusual activity patterns that traditional signature-based detection may miss. | Implement comprehensive logging and behavioural monitoring strategies to detect anomalies, use deception techniques, identify lateral movements, and respond to intrusions before they cause significant damage. |
| **Increase the frequency of scans, tests, and compliance checks** | AI-driven attacks can operate continuously, adapt in real time, and exploit vulnerabilities shortly after emergence; they can learn from failed attempts and quickly adjust tactics to bypass controls, making gaps between scheduled checks highly exploitable. This may make periodic security checks (e.g., annual penetration tests or compliance audits) insufficient. | Increase the frequency of scans, tests, and compliance checks, to keep pace with dynamic threats, moving towards continuous or near-real-time monitoring when possible. |
| **Risk management and operational resilience** | | |
| **Update incident reporting and Business Continuity Processes frameworks to account for AI-assisted threats and multi-system failure** | Incident response and business continuity plans are often designed for single-system failures or linear attack progression and may not be adequate under AI-assisted highly complex | Update and regularly test incident reporting and Business Continuity Processes frameworks for AI-assisted threats and multi-system failure, ensuring coordinated response and effective recovery. Implement strong data backup |

| | | |
|---|---|---|
| | scenarios, such as the simultaneous exploitation of vulnerabilities in diverse systems. | capabilities and ensure that backups are not exposed to the same risks as primary systems. |
| **Execute periodic operational resilience testing and evolve the testing towards AI-enhanced threat scenarios** | AI-driven attacks can trigger cascading failures across interconnected systems, disrupting operations in ways that traditional resilience tests may not anticipate. | Operational resilience testing evolves to simulate AI-enhanced threat scenarios, and financial entities should test their ability to withstand AI-assisted cyber-attacks. Scalable testing frameworks may provide a structured, but flexible threat-led approach to allow for a proportional approach to resilience testing. |
| **Identify and monitor dependencies across the full ICT infrastructure** | AI-driven attacks can analyse and exploit dependencies across a financial entity's ICT infrastructure, such as software dependencies (e.g., open-source libraries, third-party APIs), infrastructure dependencies (e.g., cloud providers, DNS services) or operational dependencies (e.g., outsourced IT/SOC). | As threat actors can use AI to map these dependencies, identify single points of failure, and chain exploits for maximum impact, it is important to identify and monitor their dependencies, assess their criticality and risk, and implement measures to mitigate AI-driven exploitation. |
| **Management body accountability to evolve from periodic oversight to continuous, informed decision making** | AI-driven attacks target not only technical systems but also governance weaknesses, decision-making gaps, and risk oversight failures. Without clear accountability at their highest level, financial entities may underestimate AI-specific risks, fail to allocate sufficient resources, or lack coordinated responses to complex, automated attack patterns. | Evolvement of the management accountability should evolve from periodic oversight to continuous, informed engagement, integrating cybersecurity into strategic decisions and that sufficient resources are allocated to manage these risks. |
| **Implement automated risk monitoring and escalation procedure** | As AI-driven threats evolve rapidly, requiring real-time visibility and escalation to ensure timely response and decision-making, the frequency of risk reporting may reveal to be insufficient for detecting and mitigating AI-enhanced attacks. | Adoption of more automated monitoring processes, as well as faster and more adaptive escalation procedures, so to contain threats before they spread into wider incidents. |

| | | |
|---|---|---|
| **Evolve cybersecurity awareness to a more reactive and proactive mindset** | AI-driven attacks can generate unusual or highly complex behavioural patterns that current security tools may not be able to identify; social engineering has also evolved the ways to target and exploit financial entities' vulnerabilities. | Advance cybersecurity awareness to tackle new threats; move from a purely preventive mindset to a more reactive one, empowering staff members to detect and report anomalies as a complementary element in the cybersecurity toolbox. |