EUROPEAN CENTRAL BANK
BANKING SUPERVISION

Claudia BUCH
Chair of the Supervisory Board

To the CEO of the significant institution

SSM-2026-0301
Frankfurt am Main, 7 July 2026

Addressing AI-enabled cybersecurity threats

Dear CEO,

Rapid advancements in emerging technologies, namely artificial intelligence (AI) systems, represent pivotal changes to the cybersecurity landscape. Emerging AI models are capable of identifying software vulnerabilities and generating functioning exploits at unprecedented speed, compressing the timeline between vulnerability discovery and exploitation. These developments have potentially profound implications for the confidentiality, integrity and resilience of banks' information and communication technology (ICT) systems. This is a long-term shift in the threat landscape rather than a temporary phenomenon or a risk tied to any single tool. The increased pace and breadth of cyber threats underscore the importance of strengthening existing ICT resilience measures and accelerating efforts to mitigate vulnerabilities. While these developments do not introduce entirely new risks, they significantly amplify the speed and scale at which such risks materialise.

Responsibility for responding to the evolving cyber-risk environment primarily lies with banks' management bodies. Strategic ICT-related decisions, including ICT investments, resource allocation and ICT risk-related risk tolerance frameworks (RTFs) may need to be revisited. In particular, governance and control systems are expected to be strengthened where necessary.

The ECB emphasises 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.

The requirements set out in the Digital Operational Resilience Act (DORA)[1] remain highly relevant and valid in view of the impending change in the cybersecurity landscape. In line with these requirements, the ECB is calling on significant institutions to assess the impact of the evolving threat landscape without

1 Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) No 2016/1011.

Address
European Central Bank
Sonnemannstrasse 20
60314 Frankfurt am Main
Germany

Postal address
European Central Bank
60640 Frankfurt am Main
Germany

Tel.: +49 69 1344 0
www.bankingsupervision.europa.eu

delay, and to develop a comprehensive action plan outlining concrete measures to strengthen relevant controls, allocating the necessary resources, assigning clear roles and responsibilities, and defining timelines for implementation.

This action plan should build upon the bank's existing cyber-risk strategy and address both immediate priorities and longer-term strategic aspects. In the short term, particular focus should be placed on the following areas:

- accelerate vulnerability and patch management at scale;
- enhance monitoring, detection and AI-enabled defensive capabilities;
- verify that third-party risk management is fit for purpose in the current situation, in light of the role of ICT service providers in critical supply chains.

As part of the short-term effort, prioritising protection of perimeter technologies and internet-facing and externally exposed ICT assets, including third-party software and open-source components, is key to preparing for the rise in AI-enabled cybersecurity threats.

In addition to these short-term actions, operational and cyber resilience should be advanced through structural measures, including:

- reinforcing defence-in-depth and cyber hygiene, and modernising infrastructure by replacing or updating legacy, unsupported or end-of-life technologies;
- improving operational resilience through response and recovery mechanisms, including crisis management, as well as information sharing arrangements.

This action plan should be submitted to the respective Joint Supervisory Team (JST) by 31 October 2026. The JST will further engage with the bank to discuss the action plan and will monitor its progress. In addition, the ECB will conduct a horizontal analysis of the submitted action plans to identify trends, challenges and areas for improvement, and will share the conclusions of this analysis with significant institutions to support them in strengthening their ICT resilience. Additional industry events or workshops may be organised, as needed, depending on the outcomes of the assessments and developments in frontier AI.

The ECB remains committed to enabling supervised institutions to prioritise their efforts and focus resources on the relevant key areas. For that reason, the ECB will extend the deadline for the annual collection of the IT Risk Questionnaire from September 2026 to February 2027. Potential adjustments to other supervisory activities, such as on-site inspections or deep dives, will be considered on a case-by-case basis. These adjustments may include remediation activities associated with recommendations raised in previous supervisory activities, especially in areas that are not related to the key focus areas but require significant involvement of banks' ICT risk functions. This will be part of the ongoing dialogue between JSTs and supervised institutions.

In light of the aforementioned developments and in line with the European Systemic Risk Board's warning on "systemic cyber risks stemming from frontier artificial intelligence models"[2] also published today, the

2 ESRB warning on "systemic cyber risks stemming from frontier artificial intelligence models": https://www.esrb.europa.eu/pub/pdf/warnings/esrb.warning260625_on_systemic_cyber_risks_stemming_from_frontier_ai_models~ef424708cf.en.pdf.

ECB expects significant institutions to take immediate and proactive measures to address the increased risks. It is important to note that the responsible CERT (Computer Emergency Response Team) / CSIRT (Computer Security Incident Response Team) authorities may provide additional relevant threat intelligence and guidance which can inform institutions' defensive postures.[3] The ECB is also actively engaged in international fora such as the G7, the Basel Committee on Banking Supervision and the Financial Stability Board, promoting international coordination in addressing AI-enabled cybersecurity threats.

Lastly, the ECB would like to highlight that other emerging technologies, like the ongoing progress towards practical quantum computing, will have a significant impact on the cybersecurity landscape. The adoption of post-quantum cryptography may involve a longer time frame, but must start now and necessitates sustained, strategic investment over time. The ECB will address the emerging risk to traditional encryption methods posed by advances in quantum computing in a separate letter in due course.

Yours sincerely,

[signed]

Claudia BUCH

Encl. annexes

3 See CERT-EU (2026), "AI is changing the economics of vulnerability discovery. Defenders should adapt now", available at https://www.cert.europa.eu/blog/ai-vulnerability-discovery-defenders-must-adapt, and consider national initiatives stemming from NIS2 (Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148).

Annex 1: Details on relevant focus areas to prepare for increasing AI-enabled cybersecurity threats

As mentioned above, the requested action plan should address short and long-term areas. The requested action plan should provide information on the following focus areas (specific actions for each area are provided for consideration):

In the short term:

1. **Prioritise the protection of potential attack surfaces**
    - Identification of ICT assets, including third-party software and open-source components, is key to prioritising remediation efforts.
    - Minimisation and continuous monitoring of all internet-facing and externally exposed assets, including cloud environments, and other VPN connections to third parties, remain important elements of an effective defensive posture.
    - Prioritising perimeter technologies in the remediation efforts helps safeguard the most exposed assets, and can be followed by cloud and on-premises environments, with a particular focus on ICT critical internal systems and ICT security infrastructure.
    - In remediation planning, it is beneficial to take into account the fact that threat vectors may originate not only from external networks but also from internal sources.
2. **Accelerate vulnerability and patch management at scale**
    - Prioritised vulnerability scanning may help institutions cope better with the increasing speed and volume of vulnerability discovery. Where appropriate, this approach could be complemented by the use of AI-based tools, provided that their deployment is preceded by a thorough assessment of both their potential benefits and associated risks, and remains subject to adequate safeguards, human oversight and robust risk management.
    - Preparation for more frequent and higher-volume patching may become increasingly important as vendors and open-source communities - as well as internally developed software - identify and remediate vulnerabilities faster, requiring ICT functions to be adequately staffed.
    - ICT change management arrangements that enable rapid, risk-based remediation while maintaining operational stability can support the effective prioritisation of emergency changes, critical fixes, internet-facing systems and critical internal systems. These should also be reflected in contractual terms and service level agreements when an ICT service provider is involved.
3. **Enhance monitoring, detection and AI-enabled defensive capabilities**
    - Strengthened monitoring of application and access logs, network traffic and other indicators can improve the detection of indicators of compromise and attempted exploitation, especially across internet-facing applications, cloud repositories and critical internal systems.

4. **Strengthen governance, funding, awareness training and supply chain assurance**

    - Management bodies and senior management should assess whether current ICT budgeting, staffing, tooling and change capacity are sufficient to support accelerated patching, infrastructure updates, resilience testing, AI-enabled defence and sector-wide coordination.
    - Training and awareness for all employees, customers, counterparties, third parties and other relevant stakeholders should be commensurate to the level of risk, appropriate for individual needs and adjusted to the evolving threat landscape in order to be relevant and useful as a protective tool, including, where relevant, training and awareness for ICT security personnel and members of the ICT lines of defence.
    - Institutions remain exposed to, and fully accountable for, risks stemming from outsourced ICT services. Adequate supply chain assurance, including an understanding of third-party ICT service providers' preparedness for accelerated vulnerability disclosure and patching, remains relevant in this context.

Risk appetite frameworks should be reviewed in order to update and/or incorporate metrics, tolerance thresholds and control measures - including those related to increased patch management frequency - consistent with the evolving risk profile stemming both from the internal use of such models and from indirect exposure to them. The management body should actively provide appropriate direction and oversight to ensure the necessary consistency with the institution's strategy and risk management framework.

In addition to these short-term remediation actions, other structural measures can include the following:

5. **Reinforce defence-in-depth and cyber hygiene, modernise infrastructure**

    - A prudent security posture assumes that perimeter defences will be breached, particularly as frontier AI systems increase the speed and scale of vulnerability discovery and exploitation, including potential zero-day exploitation.
    - Segmentation and, where feasible, micro-segmentation, together with the adoption of zero-trust principles, including continuous verification of users, devices, applications, application programming interfaces (APIs) and service accounts, can support defence-in-depth.
    - Strong baseline controls remain central to effective cyber hygiene. These include accurate asset inventories, secure configuration, robust access controls with least privilege, multi-factor authentication and comprehensive logging.
    - Software development practices based on security-by-design, with appropriate consideration of secure code alongside delivery timelines, can reduce vulnerabilities before deployment.
    - AI-native and AI-assisted defensive tools can help institutions keep pace with AI-enabled threats, provided they are deployed with appropriate governance, validation and human oversight.

- Given the increased vulnerability exposure associated with legacy, unsupported or end-of-life technologies, replacing or updating these ICT systems, or providing comprehensive protection through additional controls where replacement is not feasible, can materially reduce risk.

6. **Improve operational resilience (i.e. response and recovery), including crisis management, and information-sharing arrangements**
   - Robust and regularly tested crisis management, incident response, backup, failover, restoration and recovery arrangements aligned with DORA requirements and best practices for ICT risk management, incident handling and operational resilience testing are essential in a context of higher probability of ICT-related incidents materialising.
   - Exercises covering high-speed, high-volume attack scenarios, broad compromise through zero-day vulnerabilities, ransomware or destructive attacks and supply chain or cloud service disruption can help institutions validate preparedness under more demanding threat conditions.
   - Secure frameworks for exchanging sensitive cyber information across institutions, including vulnerabilities, threat intelligence, defensive strategies and remediation approaches, can support collective resilience, leveraging existing trusted information-sharing arrangements.

While the actions outlined above focus on enhancing banks' cybersecurity and operational resilience, institutions could consider whether their broader risk appetite frameworks still adequately reflect the evolving risk landscape and inform decision-making processes related to risk acceptance, including origination policies.

Annex 2: References to international guidelines

- CERT-EU - AI is changing the economics of vulnerability discovery: https://www.cert.europa.eu/blog/ai-vulnerability-discovery-defenders-must-adapt
- ENISA - Security by Design and Default Playbook: https://www.enisa.europa.eu/sites/default/files/2026-03/ENISA_Secure_By_Design_and_Default_Playbook_v0.4_draft_for_consultation.pdf
- Singapore CSA - Advisory on Risks associated with Frontier AI Models: https://www.csa.gov.sg/alerts-and-advisories/advisories/ad-2026-004/
- Government of Canada - Frontier artificial intelligence: https://www.cyber.gc.ca/en/guidance/frontier-artificial-intelligence
- Australian Government - Frontier models and their impact on cyber security: https://www.cyber.gov.au/about-us/view-all-content/news/frontier-models-and-their-impact-on-cyber-security
- UK NCSC - Why cyber defenders need to be ready for frontier AI: https://www.ncsc.gov.uk/blogs/why-cyber-defenders-need-to-be-ready-for-frontier-ai
- UK NCSC - Preparing for a 'vulnerability patch wave': https://www.ncsc.gov.uk/blogs/prepare-for-vulnerability-patch-wave
- UK NCSC - Retaining defensive advantage in the age of frontier AI cyber capabilities: https://www.ncsc.gov.uk/blogs/retaining-defensive-advantage-in-the-age-of-frontier-ai-cyber-capabilities
- FS-ISAC - Sector Risk Advisory: Preparing the Enterprise for AI-Enabled Vulnerability Discovery: https://www.fsisac.com/hubfs/Knowledge/AI/SectorRiskAdvisory_PreparingtheEnterpriseforAI-EnabledVulnerabilityDiscovery.pdf
- FS-ISAC - Sector risk advisory on AI-Enabled Vulnerability Detection & Remediation Perspectives on Third Parties: https://www.fsisac.com/knowledge/sector-risk-advisory-ai-enabled-vulnerability-detection-remediation-perspectives-on-third-parties
- Bank of England, FCA and HM Treasury joint statement on Frontier AI models and cyber resilience: https://www.bankofengland.co.uk/news/2026/may/boe-fca-and-hm-treasury-joint-statement-on-frontier-ai-models-and-cyber-resilience
- UK CMORG - Firm Guidance for Frontier AI: https://www.cmorg.org.uk/sites/default/files/2026-06/CMORG%20-%20Firm%20Guidance%20For%20Frontier%20AI%20-%20Final%20-%20June%202026%20-%20Version%201.0%20-%20TLP%20CLEAR.pdf
- Five Eyes Cyber Security Agencies Statement: https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/4523810/five-eyes-cyber-security-agencies-statement/