BANCA D'ITALIA
EUROSISTEMA

Communication to the Market on Digital Operational Resilience and Advanced Artificial Intelligence Models

Emerging technologies, and artificial intelligence (AI) systems in particular, are transforming the cybersecurity landscape and creating new challenges due to their potential implications for the confidentiality, integrity and resilience of information systems and the information they manage, including in the financial sector.

The most advanced generation of AI models can identify software vulnerabilities and simultaneously generate methods for exploiting them, within extremely short timeframes and without the need for specific technical expertise. This significantly reduces the time interval between the discovery of vulnerabilities and their exploitation, thereby increasing the risk of successful cyberattacks.

New AI technologies may therefore widen the asymmetry between attackers and defenders, to the detriment of the latter, requiring rapid adaptation by financial entities.[1] In this new environment, strengthening digital operational resilience is not merely a compliance requirement but an essential condition for ensuring business continuity and the ability to provide reliable financial services.

In light of these developments, Banca d'Italia – in line with the European banking supervision approach and taking into account the requirements of the Digital Operational Resilience Act (DORA), which remain highly relevant in this context – calls on financial entities to promptly identify and implement the measures needed to enhance the security processes and controls protecting their systems, with the aim of strengthening their operational and cyber resilience.

[1] This communication is addressed to the following entities directly supervised by Banca d'Italia's Directorate General for Financial Supervision and Regulation: less significant banks and banking groups (including BancoPosta), payment institutions, electronic money institutions, investment firms, managers of alternative investment funds, management companies, crypto-asset service providers, issuers of asset-referenced tokens, crowdfunding service providers and financial intermediaries under Article 106.

Financial entities are required to strengthen controls in the following areas:

- **Governance**: boards and senior management must review their Risk Appetite Framework (RAF) to incorporate risks arising from frontier technologies, in line with their strategic decisions, including those concerning ICT investments and resource allocation.[2] They must promote the strengthening of governance and control systems and ensure a clear allocation of responsibilities, including for data management and security. They are also required to put in place appropriate controls over external ICT service providers, including through adequate contractual requirements to ensure effective security monitoring and patch management, and through rigorous criteria for the assessment and selection of providers. To this end, it is important that management bodies include members with adequate technological expertise, also in the field of artificial intelligence, and allocate adequate financial resources to continuous training.
- **Cyber hygiene:** in light of the threats associated with frontier AI models, financial entities must incorporate defence-in-depth[3] and cyber hygiene principles into their strategies. This includes strong authentication and authorization processes, granular access management and continuous activity monitoring. These measures must be complemented by network and environment segmentation strategies to limit the spread of potential compromises.
- **Management of ICT assets and potential attack surface**: financial entities are required to maintain complete, up-to-date and reliable asset inventories, including in response to emerging threats. Such inventories are an essential prerequisite for identifying and managing vulnerabilities and for mapping potential attack surface. When classifying assets according to their criticality, financial entities must take into account exposure to the internet and the use of cloud-based infrastructure. At the same time, they must modernize infrastructures by replacing legacy technologies.
- **Vulnerability and patch management**: financial entities must rapidly identify vulnerabilities in their ICT systems, including through the adoption of more advanced

[2] Should a financial entity decide to adopt AI-based defensive tools (see below), their use must be consistent with its AI strategy and supported by an appropriate assessment of the specific risks associated with these technologies, as well as by the implementation of suitable safeguards (e.g. performance and model degradation monitoring, and human oversight).

[3] This refers to a cybersecurity strategy based on multiple overlapping layers of security controls. If one layer is breached, the subsequent layers intervene to stop the attack, detect the intrusion and protect sensitive data.

vulnerability-scanning techniques and, where appropriate,[4] through the use of AI-based systems, in order to reduce the gap with potential attackers. Vulnerability-management processes must be made efficient through the timely implementation of remediation measures, prioritizing the most critical issues. The focus should be on securing open-source software and systems directly accessible from the outside, particularly where vulnerabilities (including zero-day vulnerabilities) may be exploited by malicious actors.

- **Monitoring, detection and defensive measures**: financial entities must strengthen monitoring and defence systems for applications, access management and network traffic, including traffic to and from third-party ICT service providers. Where appropriate, these systems should be integrated with AI-based tools capable of analysing large volumes of data and identifying anomalies in real time, particularly with respect to critical ICT assets. Monitoring systems must also be synchronized with ICT asset inventories to ensure that assets are monitored according to their criticality classification.
- **Testing activities**: digital operational resilience testing,[5] as well as the testing of response and recovery processes, must be strengthened. Crisis-management activities should be systematically incorporated into testing programmes through the periodic assessment of operational procedures, in line with DORA requirements. Testing activities must include simulations of realistic and increasingly complex scenarios that reflect the ongoing evolution of the cyber-threat landscape resulting from technological change. These activities are becoming increasingly important in assessing an entity's preparedness in an environment where the likelihood of ICT incidents has increased.

The growing reliance on external providers increases vulnerabilities associated with the management of technological resources. Multi-layered supply chains concentrated among a limited number of operators can turn localized disruptions into widespread issues.

[4] The assessment must take into account costs and benefits, as well as an entity's overall risk profile, the complexity of its services, and the nature and scale of its activities and operations (see Article 4(1) of DORA).

[5] Reference is made in particular to: i) Article 24(1) of DORA, which requires financial entities to maintain a sound, comprehensive and up-to-date digital operational resilience testing programme as an integral part of their ICT risk management framework; and ii) Article 25(1) of DORA, which provides that 'the digital operational resilience testing programme ... shall provide ... for the execution of appropriate tests, such as vulnerability assessments and scans, open source analyses, network security assessments, gap analyses, physical security reviews, questionnaires and scanning software solutions, source code reviews where feasible, scenario-based tests, compatibility testing, performance testing, end-to-end testing and penetration testing'. In addition to these requirements, which apply to all financial entities, the provisions on Threat Led Penetration Testing (TLPT) continue to apply to entities identified by the competent supervisory authorities.

External providers must therefore support financial entities' efforts and share responsibility for ensuring the protection and continuity of systems.[6]

The financial entities' Boards of Directors are expected to review the contents of this Communication in a joint meeting with their Boards of Auditors, during which they must initiate the preparation of a report. This report will describe the current level of risk exposure and the adequacy of existing controls for each of the areas identified above, identify the main weaknesses and intervention priorities, and set out an action plan specifying the measures, timelines and investments required. The plan must be proportionate to the financial entities' risk profiles, the complexity of their services, as well as their activities and operations. It must also specify how the Boards will monitor implementation progress. Each financial entity must designate a specific internal function (for example, the second-line ICT risk control function) and notify Banca d'Italia accordingly. The report, together with the action plan, must be submitted to Banca d'Italia's Directorate General for Financial Supervision and Regulation by 31 December 2026.

[6] Banca d'Italia, *The Governor's Concluding Remarks for 2025*, 2026.