BANCA D'ITALIA
EUROSISTEMA

From Analysis to Action: AI in Financial Markets*

Closing remarks by Chiara Scotti
Deputy Governor of Banca d'Italia

OECD-EC-Banca d'Italia
Strengthening the regulatory and supervisory framework and market practices for the use of artificial intelligence in the Italian financial markets

Rome, 24 April 2026

The report[1] that underpins today's discussion is the result of a joint effort between the OECD, the European Commission and Banca d'Italia to better understand how artificial intelligence (AI) is being adopted in the Italian financial sector, with a particular focus on financial markets. The report combines a mapping of current practices with a cross-country perspective in order to identify emerging trends, the main challenges faced by market participants and public authorities, and a range of high-level policy considerations.

Beyond its analytical dimension, the report is intended to provide a structured basis for policy reflection, highlighting areas where further clarity, coordination and capacity-building may be needed to support a sound and effective adoption of AI.

Against this background, I will briefly highlight the main messages that emerge from the report and today's discussion and then focus on the areas where further attention and action appear most needed.

What the evidence shows – and why it matters

Artificial intelligence is no longer just a future prospect for finance. Its use is becoming increasingly significant across the Italian financial sector, and it is gradually extending into financial market activities. Much of this use remains concentrated in ancillary functions, internal processes and decision-support tools. At the same time, it is beginning to influence how core market functions operate.[2]

---

* I would like to thank Mauro De Santis, Giuseppe Grande and Giorgio Merlonghi for their assistance in preparing this text.

1 OECD, 'AI in Italian Financial Markets', April 2026. The report is available both in English and Italian.

2 OECD, 'Artificial Intelligence, Machine Learning and Big Data in Finance', August 2021. ESMA, 'AI adoption and trends in securities markets: EU evidence', February 2026.

This matters for a simple reason. Financial markets and infrastructures are systems in which innovation, efficiency and trust must evolve together. Changes in how information is processed or decisions are made can directly affect price formation, liquidity provision, and market integrity.[3] AI is already present in these systems today, but largely as a tool for increasing efficiency in specific functions.[4]

The challenge is not primarily technological. In many respects, the technology is advancing faster than the institutional frameworks around it. The key question is how AI can be embedded in governance, accountability, data quality, operational resilience, and the management of third-party dependencies in ways that strengthen, rather than weaken, market functioning. This also calls for public authorities and market participants to adapt their capabilities to a changing environment.[5]

Three areas where action is most needed

The report, and today's discussion, have helped bring into sharper focus three areas that are especially important for the period ahead.

Stronger shared foundations

AI cannot scale up safely or effectively in a fragmented and opaque environment. This means, first of all, reducing data gaps and promoting greater clarity and simplification in the regulatory environment.

Data are a fundamental part of the infrastructure that enables AI.[6] Improving visibility across the full adoption landscape[7] – including market maturity, institutional practices and supply chain dynamics – is essential both for effective oversight and for responsible deployment. At the same time, the availability of high-quality datasets remains a precondition for training, testing and validating models responsibly.[8]

Regulatory clarity is the other side of the same coin. Specifically, further clarification and simplification of the interaction between the AI Act and financial sector legislation remain essential to reduce uncertainty, avoid unnecessary overlaps and support a framework for adoption that is more coherent, proportionate and conducive to innovation.

---

3 FSB, 'The Financial Stability Implications of Artificial Intelligence', November 2024.

4 Scotti C., 'Journey to the future of the financial system', 31st Congresso Assiom Forex, Turin, February 2025.

5 Signorini L. F., 'Artificial Intelligence in Finance', G20 Roundtable on AI in Finance, Durban, July 2025.

6 Cf. 2.

7 FSB, 'Monitoring Adoption of Artificial Intelligence and Related Vulnerabilities in the Financial Sector', October 2025.

8 Cf. 2.

The European dimension is central on both fronts. Initiatives, such as the European Financial Data Space,[9] will be increasingly central in reducing fragmentation and supporting safe innovation at scale.[10] Consistency in AI rules, data standards and supervisory approaches is also important for the development of a truly integrated Europe-wide financial market. Excessive divergence would not only increase compliance costs, it would also limit the ability of institutions to scale AI solutions across borders and could risk fragmenting markets rather than deepening the Single Market.[11]

More effective AI governance and resilience

The second area concerns governance. Responsibility for AI must sit where authority actually resides, i.e. with boards and senior management, which should define the strategy, oversee implementation and ensure that AI-related risks are embedded in existing control frameworks.

This matters especially in financial markets, where automated processes may influence trading behaviour, liquidity provision and price formation, and where interactions among participants can amplify both efficiencies and risks. In these areas, the quality of governance is not a secondary issue; it is central to the sound functioning of markets.

The governance challenge is also closely linked to resilience. As AI becomes more dependent on complex infrastructures, external providers and data-intensive processes, operational and cyber vulnerabilities may spread more quickly and less visibly across the system.[12] This makes third-party dependencies, model risk and cyber resilience particularly important, especially where critical market functions or infrastructures are involved.

Governance frameworks will need to become more effective. Boards should take ownership of AI strategies and risk frameworks,[13] ensuring they reflect AI-specific exposures, including third-party arrangements that, while seemingly inconsequential, can silently propagate risk across the system. Operational resilience frameworks will also need to evolve and become more forward-looking. AI-related scenarios should be systematically

---

9 The European Financial Data Space (EFDS) is an EU initiative aimed at creating a common, secure infrastructure for sharing and using financial data across the EU. It forms part of the broader European Data Strategy and is designed to support AI innovation, improve supervisory data quality and strengthen the integration of EU financial markets. See: European Commission (2020), European Data Strategy; OECD, 'AI in Italian Financial Markets', April 2026.

10 OECD, 'The Interplay between Artificial Intelligence and Open Finance: Synergies, Interdependencies and Policy Implications', 2026.

11 Panetta F., 'Trade and Finance in a Fragmented World', 32nd Congresso Assiom Forex, Venice, February 2026.

12 G7 Cyber Expert Group, 'Statement on Artificial Intelligence and Cybersecurity', September 2025.

13 Cf. 2.

integrated into resilience testing. DORA[14] and TIBER-EU[15] provide the architecture, but the scenarios must reflect the actual threat landscape, from compromised training data to adversarial inputs[16] and model manipulation.[17] Over time, improved monitoring and reporting of AI-related incidents, including near misses,[18] will also become important in strengthening supervisory learning. Public authorities, for their part, will need to continue developing relevant skills and tools,[19] as Banca d'Italia is doing.

Effective governance should not be seen as a constraint on innovation, but a condition for making it sustainable and trustworthy. In finance, trust is a particularly valuable asset.

Moving from experimentation to integration

The third area concerns the transition from experimentation to integration. Italy's financial sector is making genuine progress in piloting AI applications, including in areas linked to the market value chain – from trading and portfolio management to post-trading infrastructures and advisory services.[20]

The next step is to embed AI into business processes in a way that is sustainable, well-governed and competitive. This requires clearer pathways from pilot to production, broader involvement across the ecosystem and sustained investment in the tools and competences needed to manage increasingly complex systems.

This is also where the innovation ecosystem matters. Italy already has a set of innovation facilitators, institutional channels and points of dialogue. The challenge now is to make better use of these instruments by making them more effective and more accessible to smaller firms and new entrants, which often face the greatest

---

14 Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector (Digital Operational Resilience Act – DORA). Official Journal of the European Union, L 333, 27 December 2022.

15 ECB, European Central Bank (2018), 'TIBER-EU Framework: How to Implement the European Framework for Threat Intelligence-Based Ethical Red Teaming', May 2018, updated January 2025. In 2022, Banca d'Italia, Consob and IVASS jointly adopted the TIBER-IT national guide in 2022, promoting voluntary Threat-Led Penetration Testing (TLPT) across the Italian financial system. As of January 2025, DORA (Regulation (EU) 2022/2554, Article 26) has made TLPT mandatory on a periodic basis for significant financial entities, as further specified in Delegated Regulation (EU) 2025/1190 of 13 February 2025 (RTS on TLPT). The TIBER-IT guide was updated to version 2.0 in November 2025 to align with DORA and the revised TIBER-EU framework, serving as the reference for both mandatory and voluntary tests (Banca d'Italia, Consob and IVASS, 'Guida Nazionale TIBER-IT v2.0', 2025). For a policy perspective on the TLPTs, also in light of the DORA regulation, see Scotti C., 'Threat-led penetration testing: from TIBER-IT to the DORA rules', Conference on 'Threat-Led Penetration Testing', Banca d'Italia, Rome, February 2025.

16 NIST, 'Artificial Intelligence Risk Management Framework (AI RMF 1.0)', National Institute of Standards and Technology, January 2023.

17 Cf. 2.

18 FSB, 'Format for Incident Reporting Exchange (FIRE) – Final Report', April 2025.

19 A comprehensive account of the current state of progress across OECD countries can be found in: OECD, 'Supervision of artificial intelligence in finance – Challenges, policies and practices', OECD Artificial Intelligence Papers, No. 54, 2026.

20 Panetta F., 'Finance and Innovation for the Future of the Economy'. Assemblea ABI, Rome, July 2025.

constraints. Here, too, capabilities remain a common bottleneck. Building AI expertise within institutions and authorities alike – through training, innovation facilitators, SupTech investment, and cross-border knowledge sharing[21] – is an essential condition for further progress.

Taken together, these areas set out a clear direction. The objective is not AI adoption as an end in itself, but adoption that strengthens the efficiency, resilience and competitiveness of Italian and European financial markets and infrastructures.

Concluding thoughts

Let me close with a reflection on what I believe is at stake.

The effective and responsible adoption of AI will depend on the ability of financial institutions to embed these tools into their core activities as part of sound arrangements for governance, resilience and accountability. The issue is not whether to pursue innovation or safety, but how to ensure that the two evolve together. In the near term, this requires moving beyond experimentation and strengthening the conditions for reliable scaling, including appropriate testing, transparency and risk-management practices. Public authorities, for their part, will need to continue supporting this process through guidance, oversight and by creating the conditions for safe adoption.

This also calls for a focus on more autonomous and agentic AI systems, which may increase the speed and scale with which vulnerabilities are identified or exploited. In tightly interconnected financial markets, the effects may extend more easily beyond individual institutions, reinforcing the need for preparedness, timely responses and the inclusion of AI-related scenarios into resilience frameworks. At the same time, this is not a wholly new category of risk, but an intensification of the risks already covered by existing ICT and cyber resilience frameworks. That is why compliance with DORA, together with continued supervisory dialogue and information-sharing, remains essential.

There is also a broader European dimension to this effort. If differences in rules, data standards or supervisory approaches remain too marked, the risk is not only slower adoption, but also greater fragmentation. A more coherent framework can instead help institutions scale AI solutions across borders and support a more extensive integration of the Single Market.

More generally, the quality of outcomes will depend on technology, as well as on the quality of frameworks, the range of skills and competences and the forms of cooperation through which AI is governed. Today's discussion has confirmed that the analytical basis is sound and that the direction of travel is clear.

---

21 Cf. 2.

Designed by the Printing and Publishing Division of Banca d'Italia