DIGITAL OPERATIONAL RESILIENCE - ITALY ADAPTS TO THE DORA REGULATION

With Legislative Decree no. 23/2025, which represents an important step forward in the modernisation of the Italian regulatory framework for digital security in the financial sector, Italy is now fully complying with Regulation (EU) 2022/2554 (*DORA - Digital Operational Resilience Act*), which introduces a standardised approach at European level to strengthen the resilience of digital infrastructures in the financial sector.

Below is an analysis of the main elements of the decree, with some brief considerations.

1. ICT risk management

Financial institutions must equip themselves with an ICT risk management system that is integrated into the company's governance and updated according to the evolution of threats. The obligation is not limited to protection from cyber attacks, but imposes a cultural change, requiring that digital security be considered an integral part of the business strategy, with the direct involvement of management and control bodies. The obligation is based on a principle of proportionality, providing that it is commensurate with the size and complexity of the entities concerned.

2. Reporting of significant incidents

The decree requires the timely communication to the competent authorities as well as to CSIRT Italia (*Computer Security Incident Response Team*, a body of the National Cybersecurity Agency) of any ICT incident that has a significant impact on services, customers or systems, thus strengthening the transparency and responsiveness of the financial system. The reporting obligation also contributes to building a centralised database of threats and vulnerabilities that can be useful at a systemic level to prevent future attacks.

3. Digital operational resilience testing

Entities must carry out regular audits and simulations, including Threat-Led Penetration Testing (TLPT), particularly for critical infrastructures. This is a proactive, not reactive, approach: the objective is not only to react to attacks, but to predict, simulate and anticipate them. A paradigm shift in the approach to cybersecurity in the financial sector.

4. Risk management related to third-party ICT suppliers

The decree imposes specific obligations for the management of relationships with third-party providers of technological services, including cloud, software, and platforms. In a context in which more and more institutions are outsourcing fundamental components of their infrastructure, the legislator recognises that the security chain is only as strong as its weakest link, and introduces measures to strengthen it.

5. Strengthening of supervisory authorities

The Bank of Italy, Consob and IVASS obtain new inspection and sanctioning powers to ensure compliance with the new DORA rules. European harmonisation requires that national authorities also be adequately equipped, in order to ensure more effective supervision, with appropriate tools to intervene even in complex or cross-border situations.

6. Scope of application

The rules apply to a very wide range of subjects, from traditional banks to cryptocurrency companies, reflecting the evolution of the financial ecosystem, which today includes many so-called digital native players. The decree thus avoids the risk of regulatory 'grey areas', ensuring that all operators are subject to minimum standards of resilience.

7. Sanctions and corrective measures

The decree provides for administrative sanctions, including fines, graduated according to the severity of the violation and the damage caused. The new sanctioning system, clear and proportionate, guarantees the effectiveness of the new provisions. The sanctions are also an incentive for companies to invest in security and prevention, rather than risking economic and reputational damage.

8. Conclusions

In conclusion, the decree does not merely constitute a formal adaptation to the European law: it introduces a real step change in the management of digital security in the Italian financial sector. In a context characterised by increasing digitisation and sophistication of cyber-attacks, operational resilience is no longer a choice but a necessity. The new regulations aim not only to protect individual companies, but also to safeguard the stability of the entire financial system, while strengthening users' trust in digital services.

Paolo Iemma, Partner
Email: *paolo.iemma@grplex.com*