BANCA D'ITALIA
EUROSISTEMA

Threat-led penetration testing: from TIBER-IT to the DORA rules

Opening remarks by Chiara Scotti
Deputy Governor of Banca d'Italia*

Carlo Azeglio Ciampi Conference Centre
Rome, 27 February 2025

Ladies and Gentlemen,

there is no doubt that digital resilience is a cornerstone of a stable financial system, especially as cyber attacks are increasing both in frequency and severity around the world: between mid-2023 and mid-2024, around 11,000 cyber incidents were reported globally, with more than half occurring in Europe.[1] According to the IMF, about 20 per cent of cyber incidents target the financial sector.[2] The number of incidents classified as severe – based on their economic impact, scale, duration, or the degree to which critical data or infrastructure are compromised – has also surged. The hardest-hit sectors are healthcare (about 18 per cent), defence (13 per cent) and the finance and insurance industry (8 per cent).[3] The financial sector is particularly vulnerable, not only because of the high potential profits to be made from these attacks, but also because of the vast troves of sensitive data stored by financial sector operators. In a digital economy, these data are a strategic asset.

Italy has also seen a sharp rise in these incidents. According to the Italian national cybersecurity agency (Agenzia per la Cybersicurezza Nazionale, ACN), the number of reported cyber incidents went from 126 in 2022 to 303 in 2023.[4] Similarly, the number of significant incidents reported to Banca d'Italia increased by 160 per cent in 2023

---

* I would like to thank Luca De Angelis and Antonino Fazio for their contribution to this speech.

1 EU Agency for Cybersecurity (ENISA), *ENISA Threat Landscape 2024*, 2024.

2 International Monetary Fund (IMF), *Global financial stability report*, 2024.

3 According to the 2024 report of the Italian Cybersecurity Association (CLUSIT), the average number of incidents per month doubled between 2019 and 2024, from 139 to 273. On average, nine serious cyber incidents occur every day, with roughly 90 per cent driven by financial motives (cybercrime and/or fraud). The main types of cyber threats are: (*i*) malware e ransomware (34 per cent); (*ii*) the exploitation of technological vulnerabilities (14 per cent); and (*iii*) phishing (8 per cent).

4 See National Cybersecurity Agency (ACN), *Annual Report to Parliament* (only in Italian), 2023, or its abridged version in English, *2023 Year in Review*, 2023.

compared with the previous year,[5] and early estimates point to a 30 per cent rise in 2024.

These figures underscore the urgency of investing in cybersecurity testing, including in terms of evaluating the effectiveness of the defences set up by operators. Threat-led penetration testing (TLPT) plays a pivotal role in this respect. Under the Digital Operational Resilience Act (DORA), TLPT is now mandatory for financial institutions classified as 'critical'.[6] The Eurosystem's TLPT methodology, known as threat intelligence-based ethical red teaming (TIBER-EU),[7] has been transposed in Italy by Banca d'Italia, CONSOB and IVASS into the TIBER-IT framework.[8]

To reflect the significance of this joint effort, today we have brought together representatives from the authorities, the financial sector and the cybersecurity service market. Together, we will discuss how TLPT and TIBER-IT have been applied over the past two years, the insights gained, and what lies ahead. Before we begin the day's sessions, I would like to highlight three key points: 1) the cross-cutting role of testing in strengthening cybersecurity defences; 2) the lessons learned from TIBER-IT testing in Italy; and 3) the growing importance of third-party risk.

1. The cross-cutting role of testing in cybersecurity

The EU authorities have long taken up the challenge of strengthening the Union's cybersecurity posture. To this end, they have drawn up guidelines that require financial entities – including banks, payment institutions and e-money institutions – to put in place specific safeguards.[9] Recently, DORA introduced a new regulatory framework based on five pillars:

1. ICT risk management;
2. cyber incident reporting;
3. operational resilience testing, including TLPT;
4. ICT third-party risk management, including the oversight of critical ICT providers; and

---

5 When an incident occurs, operators classify it as 'significant' if it meets the criteria and thresholds set by Banca d'Italia (based on the type and size of the financial intermediary) and report it promptly. See Banca d'Italia, 'Digital resilience in the Italian financial sector: evidences from the supervisory incident reporting framework', 2024, and Paolo Angelini, 'Cybersecurity in the financial sector: role of authorities and value of cooperation', 2024.

6 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) 2016/1011.

7 See the dedicated page on the European Central Bank's website.

8 See the dedicated page on Banca d'Italia's website.

9 See European Banking Authority (EBA), 'EBA Guidelines on ICT and security risk management', 2019. These guidelines have long been incorporated into the supervisory instructions issued by Banca d'Italia. See European Insurance and Occupational Pensions Authority (EIOPA), 'Guidelines on information and communication technology security and governance', 8 October 2020. See European Securities and Markets Authority (ESMA), *Final Report on guidelines on outsourcing to cloud service providers*, 2020.

5. information sharing, especially on major threats.

Specifically, DORA requires financial entities to integrate a testing programme into their operational digital resilience framework. This includes various tools, such as vulnerability and network security assessments, software analysis, and penetration testing. For a subset of critical players, identified using both quantitative and qualitative criteria, DORA mandates that advanced testing – namely TLPT – be performed at least every three years. Regardless of their size, though in accordance with the principle of proportionality, DORA requires all financial entities to adopt minimum cybersecurity standards and to strengthen their ability to respond to IT system crises.

Within this integrated framework of safeguards, testing serves the purposes of verifying the effectiveness of the security measures and the related operational processes, improving the ability to detect, prepare for, and respond to operational incidents and cyber attacks over time. As an operational resilience testing tool, TLPT goes beyond identifying technical vulnerabilities: it tests an organization's digital resilience, spanning systems, processes, people and providers. By cutting across all five pillars of DORA, it promotes a proactive and systemic approach to security, contributing to the stability of the entire financial sector.

The implementation of DORA has required a coordinated effort across Europe to define technical regulatory standards. The TLPT standards – which are particularly relevant to today's topic – were recently adopted by the European Commission and are currently under review by the European Parliament and the Council. We do not foresee any major hurdles or revisions, so the legislative process should be completed by the end of May.

2. TIBER-IT: methodological framework and key lessons from Italy

As I mentioned before, the Eurosystem developed the TIBER-EU methodology for conducting TLPT as early as 2018. This has ensured a harmonized approach to testing in the context of the implementation of the cyber resilience strategy for market infrastructures.[10] TIBER-EU has now been adopted by 16 European countries[11] and used in over 100 tests, reflecting the interest from operators who see it as a valuable tool for testing the security of their systems. DORA's provision for mandatory TLPT using the TIBER-EU methodology is therefore not something completely new in Europe.

Italy, too, has been moving decisively in this direction for quite some time: in 2022, the adoption of the TIBER-IT National Guidance gave Italian financial institutions the

---

10 Banca d'Italia contributed significantly to the development of this strategy and its supporting tools. In 2022, it took over the coordination of the task force responsible for updating the strategy, which was recently published. See the dedicated page on the European Central Bank's website.

11 Austria, Belgium, Denmark, Finland, France, Germany, Iceland, Ireland, Italy, Luxembourg, Netherlands, Norway, Portugal, Romania, Spain and Sweden. In addition, the ECB applies the framework at supranational level.

opportunity to undergo advanced cybersecurity testing on a voluntary basis.[12] Since then, Banca d'Italia has overseen voluntary testing for 12 entities, including banks, insurance companies and other payment system operators. These first tests have confirmed the framework's validity and value and have uncovered significant technical, procedural and organizational vulnerabilities for the entities being tested.

From a technical standpoint, they have highlighted the ability of the entities undergoing the testing to block malicious actions at the outer perimeter. However, they have also revealed weaknesses in countering intrusions after a breach has occurred, underscoring the need for security by design and to adopt defence-in-depth principles. Identity and access management practices also stood out as areas for improvement.[13]

At process level, useful indications have emerged in terms of trying to strike the right balance between the number of critical functions to be tested and the resources to be allocated by operators and providers.

At organizational level, the tests have pointed to the fact that the composition of the 'control team' responsible for the entire testing process must be carefully thought out to ensure the effectiveness, confidentiality and control of the testing. This requires the team to be made up of, at a minimum, the heads of the main corporate functions involved: IT security, business continuity and risk management.

The entry into force of DORA has made it necessary to update the TIBER-EU methodology[14] to bring it in line with the new technical standards on TLPT, especially for the components relating to the use of internal testers and the timing of the process – above all for the preparation and closure phases. In keeping with this, the national versions of TIBER, thus also our TIBER-IT, are now being revised accordingly. The experience gained from the tests conducted so far and their results will certainly help in this respect. Specifically, it will be crucial to continue to ensure that voluntary testing remains possible for all operators not subject to mandatory testing under DORA, with an eye to the cyber resilience of the system as a whole.

3. TLPT and the importance of third-party risk

A final aspect I would like to focus on is the increasing importance of third-party risk. The digitization of the financial system has led to a sharp increase in the number of functions, activities and technical-operational procedures that supervised intermediaries outsource to third-party technology providers. According to a recent analysis carried out by the European supervisory authorities in preparation for DORA, about 3,500 operators reported having 25,000 contracts with around 10,000 providers.[15] As part of Banca

---

12 See Luigi Cannari, 'La resilienza cibernetica del sistema finanziario italiano: il ruolo dei test TIBER-IT' (Cyber resilience of the Italian financial system: the role of TIBER-IT tests – only in Italian), 2022.

13 For example, through greater use of multi-factor authentication.

14 See the dedicated page on the European Central Bank's website.

15 See EBA, EIOPA, ESMA, 'ESAs workshop on DORA dry run lessons learnt and data quality', 2024.

d'Italia's supervisory activities, Italian financial intermediaries reported having more than 5,000 contracts relating to the outsourcing of key functions.[16] These providers are often completely outside the financial industry and serve a broad range of economic, manufacturing and service sectors. In many jurisdictions, they are subject to little or no oversight compared with the financial sector operators to which they provide services.[17]

Cyber resilience, therefore, also depends on the robustness of technology providers. They are a key element of the system which requires special attention, as shown by a number of incidents, including recent ones, that in some cases were malicious and in some other cases were not. Among the malicious incidents, let us cite the ransomware attacks on an Italian provider of document management and communication services, whose customers include many financial players, and on an international provider of services supporting securities trading and settlement. In addition, there have been some recent major operational incidents unrelated to cyber attacks, such as the CrowdStrike and Worldline cases last year.

An innovative aspect of DORA is precisely the regulator's focus on third-party risk management, particularly with respect to 'critical third parties' as defined based on qualitative and quantitative indicators and financial sector interdependencies.

A special case is constituted by the external providers involved in TLPT, particularly in terms of two specific types of cybersecurity services: cyber threat intelligence[18] and red teaming.[19] In order to minimize the risks inherent in the testing of systems in the production environment, it is necessary to ensure the quality and reliability of these providers. In this regard, the TIBER-EU methodology and the DORA Regulation lay out a number of requirements for the procurement of the aforementioned services by operators: the assessment of previous experience, technical skills and certifications, having professional insurance, and adhering to codes of ethics. Providers are also required to adopt strict security measures, as they themselves are potential targets for attackers interested in accessing sensitive information.

During today's conference, we will present the results of a survey on the provision of cybersecurity services in Italy, conducted last year and aimed at outlining the main characteristics of the companies operating in this sector, with a specific focus on TLPT-related services. The results point to the great dynamism of this branch of the industry, marked by soaring turnover, the presence of many new companies, and frequent changes in company structures. It is interesting to note that about 70 per cent of the respondents stated that they are currently providing or would like to provide TLPT-related services, and the share is higher for large companies.

---

16 See Banca d'Italia, *Annual Report for 2023*, 2024.

17 See Financial Stability Board (FSB), 'Enhancing Third-Party Risk Management and Oversight', 2023.

18 'Cyber threat intelligence' refers to information on threats that has been aggregated, processed, analysed, interpreted or enriched to provide the necessary context for decision-making processes. See FSB, 'Cyber lexicon', 2023.

19 'Red teaming' refers to a controlled simulation of an attack conducted by an independent group (the red team) using the tactics, techniques and procedures of real-world threat actors.

4. Conclusions

TLPT represents a unique opportunity to strengthen the resilience of the financial sector. It is in this spirit that all players, including those that do not specifically fall within the scope of DORA's provisions, should take a proactive approach to cyber threat management and voluntarily adopt the TIBER-IT framework made available by the supervisory authorities. These tools should not be seen as a mere regulatory requirement, but as an actual investment in the digital resilience of organizations and of the entire financial system.

In this regard, going forward, I would like to mention three key points: the cost of testing, the availability of skilled staff, and the opportunity offered by supranational coordination.

Developing the market for these services would contribute to greater competition, cost optimization and test quality, making TLPT accessible to a higher number of operators.

Collaboration between the supervisory authorities, academia, and the financial and ICT services industry has the potential of fostering the emergence of staff with cybersecurity skills, thus expanding the availability of professionals specialized in the services needed for TLPT.[20]

Finally, better coordination between European financial authorities would help prevent TLPT from becoming overly burdensome, especially for Pan-European operators or those providing financial services to multiple players. Where appropriate and as provided for in the regulations, joint testing between several operators should be encouraged.

---

20 See Alessandra Perrazzelli, 'Cyber sicurezza: Una continua sfida per l'economia e per la società' (Cybersecurity: A continuous challenge for the economy and for the society – only in Italian), 2023.

Designed by the Printing and Publishing Division of the Bank of Italy