Internal Security Review
2026, no. 34, pp. 237–258

https://doi.org/10.4467/20801335PBW.26.011.23373

ARTICLE

Threat-led penetration testing (TLPT) – a new approach to testing digital resilience of financial entities in Poland in the perspective of requirements under the Digital Operational Resilience Act (DORA)

KAMIL MROCZKA

Faculty of Political Science and International Studies,
University of Warsaw

https://orcid.org/0000-0003-3809-3479

PAWEŁ PIEKUTOWSKI

Cybersecurity Department,
Polish Financial Supervision Authority

https://orcid.org/0009-0001-5861-7367

Abstract

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) launched a new model for testing the digital resilience of financial services operating in the Polish financial market into the EU and thus into the domestic legal framework. The primary purpose of this article is to discuss and evaluate the Threat-Led Penetration Testing (TLPT) model. TLPT tests can include both technical and sociotechnical components. The hypothesis of the article is that

TLPT testing will have a positive impact on enhancing the digital resilience of financial stakeholders because these tests are designed to simulate real-world cyber attacks, enabling organisations to understand their resilience to threats and initiate relevant countermeasures. The results obtained from the analysis confirm the validity of the proposed research hypothesis. This follows from the fact that the main premise of TLPT testing is to replicate real-world attack scenarios as accurately as possible, thereby enabling a more reliable and detailed assessment of organisation's security level. The authors emphasise that such an approach allows not only for the verification of the effectiveness of information system safeguards, but also for the evaluation of the resilience of operational processes and the level of employee awareness regarding cyber threats.

Keywords TLPT tests, DORA, Polish Financial Supervision Authority, digital resilience, cybersecurity

Introduction

Information and communication technologies (ICT) are present in almost every area of the functioning of states and their economies[1]. They provide real support for complex systems used in everyday activities. These technologies drive the Polish economy and its most important sectors, including the financial sector, and strengthen the functioning of the European Union's internal market. The increasingly dense network of interconnections between financial market stakeholders, financial service providers, and customers, together with the ongoing digitisation of financial systems, increases vulnerability to various types of risk, including those resulting from cyber threats and disruptions to the functioning of ICT. It is therefore essential to take measures to increase the digital resilience of financial entities.

Recital 2 of Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial

[1] The article draws on a publication by one of the authors prepared for the purposes of implementing the DORA regulation. See: *Testy TLPT – nowe podejście do testowania cyfrowej odporności Organizacji* (Eng. TLPT testing – a new approach to testing digital resilience of organisation), Komisja Nadzoru Finansowego, 14 VII 2025, https://www.knf.gov.pl/dla_rynku/dora/wymagania_rozporzadzenia_dora/testy_TLPT_nowe_podejscie?articleId=90547&p_id=18 [accessed: 9 II 2026].

sector (hereinafter: DORA Regulation)[2] clearly emphasises that (…) *The use of ICT has in the past decades gained a pivotal role in the provision of financial services, to the point where it has now acquired a critical importance in the operation of typical daily functions of all financial entities*. The literature rightly points out that the DORA regulation in force since January 2025 has obliged financial entities and external ICT service providers to apply best practices in the field of cybersecurity. Threat-led penetration testing (TLPT) has been identified as one of the advanced measures leading to increased digital resilience of financial entities. They will be used to assess the cybersecurity status of these entities[3].

Without going into an in-depth analysis of the meaning of the term 'threat-led penetration testing' at this point, it should be emphasised that it is a cybersecurity assessment technique used to simulate realistic cyberattack scenarios targeting an organisation's critical systems and infrastructure. Unlike traditional penetration tests, which may be based on a standard list of vulnerabilities, TLPT method focuses on mimicking specific actors, techniques and tactics that are most likely to occur in an organisation due to its unique risk profile. TLPT tests are conducted to identify weaknesses, verify existing security measures, and enhance the organisation's ability to detect, respond to real cyber threats, and recover data[4].

The main aim of the article is to critically analyse TLPT model as an instrument for assessing the digital resilience of financial entities in Poland in the context of the requirements of the DORA regulation, with particular empahasis on the differences between TLPT tests and classic penetration tests, the role of supervisory authorities and the implications for implementation.

The authors of the article adopted the following hypothesis: TLPT tests should have a positive impact on increasing the digital resilience of financial entities. They are designed to mimic real cyber attacks, which enables organisations to understand their resilience to threats and take appropriate corrective actions.

For the purposes of this study, the comparative law method, institutional analysis and critical analysis of scientific literature were used. Participant observation based on professional experience of the authors was also applied. The methods indicated the role and competences of entitites responsible for financial market cybersecurity, identified differences in approaches to digital resilience testing,

---

[2] *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.*

[3] M.L. Dozsa*, Modular Automated Cyber Range Deployment with Adversary Emulation. In Compliance with the Digital Operational Resilience Act (DORA)*, master's thesis, Oslo 2024, p. ii.

[4] B. Riaz, Z. Younas, *Investigating the impact of DORA Regulations on Third Party Risk Management in the Swedish Financial Sector*, Stockholm University 2024, p. 26.

assessed the degree of regulatory harmonisation, and highlighted areas where the Polish model of financial market cybersecurity supervision may need to be clarified or further developed.

TLPT testing – definition

When defining TLPT testing, cybersecurity experts empasise that this is (…) *an advanced form of penetration testing that goes beyond the standard approach, simulating real cyber attacks using tactics, techniques and procedures (TTP) employed by real cybercriminals. Unlike traditional penetration testing, TLPT focuses on analysing the specific threats to which an organisation is exposed, tailoring attack simulations to its specific risk profile*[5].

The legal definition of TLPT tests is contained in Article 3 point 17 of the DORA regulation. According to this provision the testing means (…) *a framework that mimics the tactics, techniques and procedures of real-life threat actors perceived as posing a genuine cyber threat, that delivers a controlled, bespoke, intelligence-led (red team) test of the financial entity's critical live production systems*[6].

Penetration testing and TLPT testing – the most important differences

The main objective of the tests is to assess the institution's actual resilience to threats and possible attack scenarios. The penetration test focuses more on identifying technical vulnerabilities and configuration errors in IT systems.

To be more specific, the following differences can be identified:

1) scope of test implementation – penetration tests typically focus on specific elements of the IT infrastructure – individual systems, applications or network components. Their primary goal is to detect technical vulnerabilities in a defined area. This approach allows for an assessment of the security of a specific system, but does not provide a complete picture of how an organisation would cope with a complex cyber attack. TLPT testing takes a much broader approach. It covers not only systems

[5] *Testy TLPT – cyfrowa odporność organizacji zgodnie z rozporządzeniem DORA* (Eng. TLPT tests – digital resilience of organisations in accordance with the DORA regulation), Bankowe ABC, 2 I 2025, https://bankoweabc.pl/2025/01/02/testy-tlpt-a-dora/ [accessed: 19 IV 2025].

[6] See also: J. Kurek-Sobieraj, Komentarz do art. 3 (Eng. Commentary on Article 3), in: *Rozporządzenie UE w sprawie operacyjnej odporności cyfrowej sektora finansowego (DORA). Komentarz*, J. Byrski, J. Kurek-Sobieraj (eds.), Warszawa 2025, pp. 85–86.

and technologies, but also operational processes and people. The aim is to examine the organisation's entire cyber defence ecosystem and answer questions like: how does security monitoring work? How does internal communication work? How does the team respond to incidents? What are the escalation paths? TLPT testing allows you to see whether your organisation is prepared for an attack not only in theory but also in practice. This makes it possible to increase the resilience of the entire 'organism' rather than just a single element;

2) attack scenarios – penetration tests are mainly based on known vulnerabilities and focus more on identifying potential threats in a specific IT system. TLPT tests are implemented on the basis of scenarios developed by a special threat intelligence team. It is intended to identify the most realistic cyber threats and attack scenarios that a given organisation may face. These scenarios may be based on reports concerning general analysis of cyber threats (generic threat intelligence) for a given sector. The report published by the Computer Security Incident Response Team of the Polish Financial Supervision Authority (KNF CSIRT) describes the potential types of attacks, categories of adversaries, and trends in cyber attacks[7]. It places great emphasis on the potential development of threats related to the use of techniques and tools based on artificial intelligence, as well as the dangers resulting from attacks on supply chains. Other important aspects include the intensification of ransomware attacks, increasingly carried out in the ransomware as a service model, and the development of hacktivism, which has gained momentum since the outbreak of war in Ukraine;
3) test environment and risk approach – penetration tests are usually carried out in appropriate test environments to avoid disruptions to system operations. TLPT tests place great emphasis on comprehensively examining the actual level of security within an organisation, which is why they are carried out in production environments. This means additional risk associated with the possibility of disrupting the continuity of systems and business processes. Therefore, during TLPT testing, it is necessary to conduct a risk analysis to mitigate any disruptions that may arise during implementation;
4) test procedure and confidentiality – a characteristic feature of TLPT tests is the requirement to keep them secret from most organisations. Only a small

[7] *Krajobraz cyberzagrożeń w polskim sektorze finansowym 2025* (Eng. The cyber threat landscape in the Polish financial sector 2025), CSIRT KNF, https://cebrf.knf.gov.pl/images/GTL_2025_FINAL.pdf [accessed: 19 I 2026].

group of employees are aware of their implementation. The intention is to verify the organisation's response to cyber threats. Not only is the digital resilience of ICT systems examined, but also the preparedness of security teams and the functioning of relevant processes within the organisation. Maintaining test confidentiality is a major challenge for the organisation due to the complexity of many business processes;

5) results and reporting – an important element of TLPT tests are purple team exercises, which take place after the attack phase. These are exercises in which the team simulating attacks and the team responsible for defence jointly discuss the scenarios carried out, identify weaknesses in the processes and systems as well as develop solutions to increase the organisation's cyber resilience. Then, a corrective action plan is prepared;
6) test frequency – penetration tests can be performed more frequently. TLPT tests are performed much less frequently due to their complexity and costs.

Obligation to test the digital resilience of financial entities in light of Article 26 of the DORA regulation

The DORA regulation obliges financial entities (with certain exceptions specified in Article 16(1), first paragraph of the DORA regulation) to conduct TLPT tests at least every three years. However, based on the risk profile of the financial entity concerned and taking into account the operational circumstances, the competent authority may, if necessary, request that entity to reduce or increase the frequency of TLPT testing. The literature states that this may occur if (…) *the competent authority has reasonable grounds to suspect that there has been improper risk management within the organisation (e.g. due to the appearance of offers to sell the organisation's data on the black market)*[8].

Paragraph 2 of the aforementioned provision is extremely important from the perspective of quality requirements. It states that: *each threat-led penetration test shall cover several critical or important functions of a financial entity or all such functions, and shall be performed on live production systems supporting such functions.* The first step towards conducting reliable TLPT tests is to identify all relevant base systems. Financial entities should then determine all ICT processes

[8] C. Cichocki, *Komentarz do art. 26* (Eng. Commentary on Article 26), in: *Rozporządzenie UE w sprawie operacyjnej odporności cyfrowej sektora finansowego (DORA). Komentarz*, J. Byrski, J. Kurek-Sobieraj (eds.), Warszawa 2025, p. 280.

and technologies that support critical or important functions. The final step is to determine which ICT services, including systems, processes and ICT technologies supporting critical or essential functions and services, have been outsourced to external ICT service providers or are covered by a contract with such providers.

The doctrine rightly emphasises that the professional process of gathering this information and data requires business knowledge about the functioning of the organisation and its translation into technological and technical knowledge. Various ICT tools can be used for such activities, e.g. CMDB systems (computer management database)[9]. In practice, the study may cover all or only selected systems or functionalities. Taking into account the high level of interdependence of systems and ICT tools across financial entities, comprehensive research is recommended. Based on the information and data obtained from the analysis, these entities are required to assess which critical or significant functions should be covered by TLPT tests. This assessment shall be approved by the competent authorities. In the Polish legal order this is the Polish Financial Supervision Authority (KNF), which will be discussed later in the article.

Where the scope of TLPT includes external ICT service providers, the financial entity shall take the necessary measures and safeguards to ensure that they participate in the tests and shall remain fully responsible for ensuring compliance with the DORA regulation at all times. This requirement is critically important in the context of how financial entities operate, as they all use the services of external suppliers.

The EU legislator, aware of the scale of ICT service providers' operations, introduces certain derogations from the general rule of their participation in TLPT tests. In accordance with the wording of Article 26(4) of the DORA regulation:

> (…) where the participation of an ICT third-party service provider in TLPT (…) is reasonably expected to have an adverse impact on the quality or security of services delivered by the ICT third-party service provider to customers that are entities falling outside the scope of this Regulation, or on the confidentiality of the data related to such services, the financial entity and the ICT third-party service provider may agree in writing that the ICT third-party service provider directly enters into contractual arrangements with an external tester, for the purpose of conducting, under the direction of one designated financial entity, a pooled TLPT involving several financial entities (pooled testing) to which the ICT third-party service provider provides ICT services.
>
> That pooled testing shall cover the relevant range of ICT services supporting critical or important functions contracted to the respective ICT

[9] Ibid.

third-party service provider by the financial entities. The pooled testing shall be considered TLPT carried out by the financial entities participating in the pooled testing.

The number of financial entities participating in such testing shall be appropriately adjusted and take into account the complexity and type of services covered. After the tests have been completed, the reports and corrective action plans have been agreed upon, the financial entity and, where applicable, the external testers shall submit to the competent authority a summary of the findings, the corrective action plans and documentation demonstrating that the tests have been carried out in accordance with the requirements of the Regulation. On this basis, the competent authorities issue a certificate to the financial entities confirming that the tests have been carried out in accordance with the requirements set out in documentation. It enables authorities to mutually recognise TLPT tests, but does not exempt financial entities from responsibility for the results of these tests.

Financial entities were required to conclude agreements aimed at carrying out TLPT tests. If financial entity has internal testing teams, the DORA regulation requires that such tests be performed by an external tester every three tests, i.e. at least every nine years. An exception to this rule applies to credit institutions classified as significant in accordance with Article 6(4) of the Council Regulation (EU) No. 1024/2013[10]. These entities are obliged to use only external testers.

The DORA regulation also defines the criteria used by the competent authorities to determine which entities are subject to TLPT testing. The assessment takes into account:

- impact-related factors, in particular the extent to which the services provided and activities undertaken by the financial entity impact the financial sector,
- possible financial stability concerns, including the systemic character of the financial entity at Union or national level,
- specific ICT risk profile, level of ICT maturity of the financial entity or the applied technological solutions.

Synthesising the objective and subjective analysis of Article 26 of the DORA regulation, it should be noted that this provision gives Member States the possibility to designate a single public authority in the financial sector which will be responsible at national level for matters relating to TLPT testing in this sector. This authority is entrusted with all competences and tasks in this area.

[10] *Council Regulation (EU) No 1024/2013 of 15 October 2013 conferring specific tasks on the European Central Bank concerning policies relating to the prudential supervision of credit institutions,* p. 63.

Requirements for external and internal testers

Article 27 of the DORA regulation defines the basic requirements for testers conducting TLPT tests. Paragraph 1 of this provision stipulates that financial entities shall only use the services of external testers who:

a) are of the highest suitability and reputability;
b) possess technical and organisational capabilities and demonstrate specific expertise in threat intelligence, penetration testing and red team testing;
c) are certified by an accreditation body in a Member State or adhere to formal codes of conduct or ethical frameworks;
d) provide an independent assurance, or an audit report, in relation to the sound management of risks associated with the carrying out of TLPT, including the due protection of the financial entity's confidential information and mitigation of the business risks of the financial entity;
e) are duly and fully covered by relevant professional indemnity insurances, including against risks of misconduct and negligence.

The doctrine rightly emphasises that (…) *the accuracy and reliability of TLPT tests is considered crucial by the legislator, as individual financial organisations should trust the certificates presented by other entities in the industry. The level of trust in external and internal testers is also important for the competent supervisory authority*[11].

EU law permits the use of internal testers. However, the legislator imposes additional requirements, apart from those mentioned above in relation to external testers. Article 27(2) of the DORA regulation stipulates that financial entities using internal testers shall ensure that the following conditions are met:

a) such use of internal testers has been approved by the relevant competent authority or by the single public authority designated in accordance with Article 26(9) and (10);
b) the relevant competent authority has verified that the financial entity has sufficient dedicated resources and ensured that conflicts of interest are avoided throughout the design and execution phases of the test; and
c) the threat intelligence provider is external to the financial entity.

Article 27(3) of the DORA regulation draws attention to issues of information and data security arising from TLPT testing. Financial entities are required to ensure that contracts concluded with external testers oblige those testers to (…) *a sound*

[11] C. Cichocki, Komentarz do art. 27 (Eng. Commentary on Article 27), in: *Rozporządzenie UE w sprawie operacyjnej odporności cyfrowej sektora finansowego (DORA). Komentarz*, J. Byrski, J. Kurek-Sobieraj (eds.), Warszawa 2025, p. 284.

management of TLPT results and that any data processing thereof, including any generation, store, aggregation, draft, report, communication or destruction, do not create risks to the financial entity.

Cezary Cichocki rightly points out that the data obtained as a result of TLPT tests should be treated as particularly sensitive, given that if it (…) *falls into the wrong hands, it will serve as a kind of guide to vulnerabilities in the financial organisation's systems and make it much easier for a potential intruder to launch an attack. The risk of disclosing this data lies in the fact that there may be a time lag between the disclosure of threats in TLPT tests and their mitigation, which could become a window of opportunity for attack if the test data is disclosed to unauthorised persons*[12].

Testing the digital resilience of financial entities under national law

The DORA regulation created a new regulatory environment for financial entities and the Polish Financial Supervision Authority, as the body responsible for supervising compliance. The provisions of the regulation are applied directly, but some of them require changes to the national legal system, especially with regard to the designation of competent authorities and the imposition of obligations on financial entities[13].

The first draft act implementing the aforementioned EU regulations was submitted by the Minister of Finance in April 2024[14]. The legislative process took over a year, which raises questions in the context of the urgency of introducing this regulation. The tardiness of decision-makers led the European Commission to call on Poland and 12 other EU countries at the end of March 2025 to fully implement the DORA regulation within national legal systems[15]. The government legislative process was completed in April 2025. The draft law amending certain laws in connection with ensuring the operational digital resilience of the financial

[12] Ibid., p. 285.

[13] *Ustawa wdrażająca DORA do prawa polskiego* (Eng. Act implementing DORA into Polish law), "Biuletyn prawny dla branży finansowej", Deloitte, https://www.deloitte.com/pl/pl/Industries/financial-services/perspectives/ustawa-wdrazajaca-DORA-do-prawa-polskiego.html [accessed: 12 IV 2025].

[14] *Draft law amending certain laws in connection with ensuring the operational digital resilience of the financial sector and the issuance of European Green Bonds*, print no. UC11, Rządowe Centrum Legislacji, Warszawa 2025.

[15] The list of countries that have not implemented the regulation also includes: Belgium, Bulgaria, Denmark, Greece, Spain, France, Lithuania, Latvia, Malta, Portugal, Romania and Slovenia.

sector has been approved by the Standing Committee of the Council of Ministers. The act implementing the DORA regulation was passed in June 2025[16].

From the perspective of the purpose of this article, the most important changes concern the introduction of Article 18zk to the *Act of 21 July 2006 on financial market supervision*. This provision regulates the tasks of the Polish Financial Supervision Authority concerning the performance of the tests referred to in Article 26 of the DORA regulation and the procedure to be followed by financial entities obliged to perform them. Pursuant to this provision, the supervisory authority became the authority responsible for performing the duties of the competent authority specified in Article 26 and Article 27 of the DORA regulation. In the light of the above, the Polish Financial Supervision Authority has been granted the statutory power to designate, by way of a decision, the financial entity responsible for conducting TLPT tests. Article 18zk replicates the criteria for selecting entities obliged to carry out these tests, taking into account the principle of proportionality (Article 4(2) of the DORA regulation).

Entities to which the Polish Financial Supervision Authority has issued the aforementioned decision are obliged to submit to the supervisory authority, for approval, the result of the assessment carried out in accordance with Article 26(2) paragraph three of the DORA regulation. This result indicates which critical or important functions should be covered by TLPT tests. After conducting them, agreeing on reports and corrective action plans, the financial entity and, where applicable, the external testers shall be required to submit to the Polish Financial Supervision Authority a summary of the findings, corrective action plans and documentation confirming that TLPT tests have been conducted in accordance with the requirements of the DORA regulation. It will be the supervisory authority's responsibility – in the light of Article 18zk(4) – to confirm this compliance. This is to enable mutual recognition of penetration tests by the relevant authorities.

The Polish Financial Supervision Authority has also been granted powers to reduce or increase the frequency of TLPT testing and the authority to approve financial entity's intention to use the services of internal testers. It is also responsible for verifying that internal testers meet the requirements of the DORA regulation. The fulfilment of this obligation – in light of the vague requirements of Article 27 of the DORA regulation – may cause significant problems. However, it can be assumed that it is in the interest of financial entities to ensure the appropriate quality of resources for conducting TLPT tests. The quality of these tests increases

[16] *Act of 25 June 2025 on amendments to certain acts in connection with ensuring the operational digital resilience of the financial sector and the issuance of European green bonds.*

the level of digital resilience and, consequently, the broadly understood security of financial entity.

Regulatory technical standards in the field of TLPT testing

In Article 26(11) of the DORA regulation, the EU legislator decided that the European Supervisory Authorities (ESA), in consultation with the European Central Bank, would develop common draft regulatory technical standards (RTS)[17] in accordance with the European framework for threat intelligence-based ethical red teaming (TIBER-EU). The following elements are to be clarified in the RTS:

- criteria used for the purpose of the application of paragraph 8, second subparagrap of the DORA regulation,
- criteria defining the methods of identification and notification of entities obliged to perform TLPT tests,
- roles and responsibilities of individual teams participating in tests,
- requirements and standards governing the use of internal testers,
- requirements in relation to:
  - scope of TLPT,
  - testing methodology and approach to be followed for each specific phase of the testing process,
  - testing stages relating to results, test closure and corrective measures,
- the type of supervisory cooperation and other relevant cooperation which are needed for the implementation of TLPT tests, and for the facilitation of mutual recognition of that testing, in the context of financial entities that operate in more than one Member State. This is to enable appropriate level of supervisory involvement and a flexible implementation taking into account specificities of financial sub-sectors or local financial markets.

In July 2024, the ESA presented the RTS consultation final report on TLPT[18].

[17] Regulatory technical standards impose detailed technical requirements for the implementation of regulations. They are more prescriptive and focus on the practical aspects of implementing the DORA regulation. In turn, implementing technical standards (ITS) are responsible for the harmonisation and standardisation of the processes for implementing these provisions in the EU and are more procedural in nature. They focus much more on the appropriate way of reporting to the relevant supervisory authorities.

[18] *Final Report. Draft Regulatory Technical Standards specifying elements related to threat led penetration tests under Article 26(11) of Regulation (EU) 2022/2554*, European Banking Authority, 17 July 2024.

TLPT and TIBER-EU tests

Before discussing the interdependencies between TLPT and TIBER-EU tests[19], it is necessary to briefly characterise the assumptions of this document. The TIBER-EU framework was established in 2018 by the European Central Bank in order to systematise and standardise the approach and implementation of realistic penetration tests in organisations from the financial sector of EU Member States[20]. TIBER-EU defines a model for red team tests/operations preceded by reconnaissance and analysis of data on threats targeting the tested entity. It is the foundation of the requirements for TLPT tests. In the initial stage there were differences between the assumptions of this document and the requirements specified in the DORA regulation. The main one concerned the approach to conducting tests with the participation of internal testers. TIBER-EU did not initially allow for this solution, and in TLPT tests it is acceptable provided that certain criteria are met. The TIBER-EU framework was updated in 2025 and its current version reflects the requirements arising from the DORA regulation[21]. It can therefore be considered that the current TIBER-EU is a textbook for TLPT tests. While the DORA regulation specifies what must be done in TLPT tests, TIBER-EU indicates how it should be done.

The TIBER-EU framework also allows for local implementation to better suit the specific nature of a given country[22]. As of April 2025, among those who decided to implement were: Austria, Belgium, the Netherlands, France, Germany, Denmark, Finland, Sweden and Norway.

---

[19] On the topic of TIBER-EU assumptions, see more: T. Valkeasuo, *TIBER-EU Preparation Phase Framework. Case study Nixu: optimizing TIBER-EU engagements*, Jyväskylä: JAMK University of Applied Sciences, March 2023; M. Bayle de Jessé, *The Eurosystem's cyber resilience strategy for financial market infrastructures*, "Cyber Security: A Peer-Reviewed Journal" 2019, vol. 2, no. 4, pp. 294–302. https://doi.org/10.69554/DFBJ2963; B.F. Scott, *Red teaming financial crime risks in the banking sector*, "Journal of Financial Crime" 2021, vol. 28, no. 1, pp. 98–111. https://doi.org/10.1108/JFC-06-2020-0118.

[20] *TIBER-EU i DORA szansą na budowanie realnej cyberodporności w sektorze finansowym* (Eng. TIBER-EU and DORA as an opportunity to build real cyber resilience in the financial sector), Z-LABS, 8 VII 2024, https://blog.z-labs.eu/2024/07/08/tiber-eu-dora-cyberodpornosc.html [accessed: 19 IV 2025].

[21] *TIBER-EU Framework. How to implement the European framework for Threat Intelligence-Based Ethical Red teaming*, European Central Bank, January 2025, https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework_2025~b32eff9a10.pl.pdf?0309990e5e167a47ca4748370a949064 [accessed: 9 II 2026].

[22] *Implementacje frameworku TIBER-EU w Europie a wdrożenie w Polsce* (Eng. Implementations of the TIBER-EU framework in Europe and implementation in Poland), Komisja Nadzoru Finansowego, 27 I 2025, https://www.knf.gov.pl/?articleId=91971&p_id=18 [accessed: 19 IV 2025].

TIBER-EU documentation includes numerous studies that may be useful during the implementation of both TLPT and TIBER-EU tests. The most important are:

- *TIBER-EU Guidance for Service Provider Procurement*[23] – a collection of best practices in the implementation of red team and threat intelligence provider service procurement processes,
- *TIBER-EU Purple-Teaming Guidance*[24] – a collection of best practices for conducting purple team exercises that take place after red team testing,
- *TIBER-EU Scope Specification Document Guidance*[25] – guidelines for the appropriate selection of the scope of tests,
- *TIBER-EU Test Summary Report Guidance*[26] – guidelines on preparing a test summary report.

Main principles of TIBER-EU:

- tests based on real threats (threat intelligence) – test scenarios that take into account current threat intelligence,
- simulation of real attacks (red teaming) – a controlled test in which red team simulates the actions of cybercriminals,
- protection of critical functions – verification of resistance to attacks on key business functions,
- cooperation and consent – financial institution voluntarily agrees to participate in the tests,
- standardisation and possibility of implementation in various EU countries – a framework model adapted at the national level,
- learning and improvement – the analysis and learning (lessons learned) phase as an important TIBER-EU element.

[23] *TIBER-EU Guidance for Service Provider Procurement*, European Central Bank, January 2025, https://www.ecb.europa.eu/pub/pdf/annex/ecb.tiber_eu_service_provider_procurement_2025.en.pdf?1d229f2191835b83770d593a44f69b14 [accessed: 19 IV 2025].

[24] *TIBER-EU Purple Teaming Guidance*, European Central Bank, January 2025, https://www.ecb.europa.eu/pub/pdf/annex/ecb.tiber_eu_purple_best_practices_2025.en.pdf?759d46ff75caf6e644af0fd757415aee [accessed: 19 IV 2025].

[25] *TIBER-EU Scope Specification Document Guidance*, European Central Bank, January 2025, https://www.ecb.europa.eu/pub/pdf/annex/ecb.tiber_scope_specification_document_guidance_2025.en.pdf?67dc9f94d617ea2522e9a3764f43b92c [accessed: 19 IV 2025].

[26] *TIBER-EU Test Summary Report Guidance*, European Central Bank, January 2025, https://www.ecb.europa.eu/pub/pdf/annex/ecb.tiber_test_summary_report_guidance_2025.en.pdf?ecc819840c37a008b908578dd1d48b50 [accessed: 19 IV 2025].

TLPT teams

As already mentioned, TLPT tests are highly complex. They require various competencies and skills from team members. It is very important to precisely define the roles, responsibilities, and duties of the people and teams involved. This increases the chance that every aspect of the test will be well managed and that subsequent activities will be carried out according to the agreed schedule. Precise definition and assignment of roles means better coordination of activities, minimisation of the risk of errors, as well as quick identification and appropriate addressing of any problem.

The basic model of division of roles, responsibilities and duties assumes the existence of the following teams:

- TLPT cyber team (TCT),
- control team (CT) also known as white team,
- blue team (BT),
- threat intelligence provider (TIP),
- red team (RT),
- purple team (PT).

TLPT cyber team – is appointed by the authorised test supervisory authority. The team is responsible for monitoring and assessing the correctness of the tests, as well as their reliable and secure execution. The team should also ensure that all aspects of the test are carried out according to plan, minimising the risk of errors and irregularities.

Control team (white team) – plays a key role as it is responsible for coordinating the implementation of tests on the financial entity's side – planning, monitoring and managing all aspects of them. Senior managers and experts with knowledge of the organisation's infrastructure and operational processes participate in CT's work. The team is also responsible for protecting the integrity and stability of production systems during testing. It is the only team that has information about the details of the tests, which allows it to objectively assess the organisation's employees' responses to simulated threats.

Blue team – is responsible for managing internal cybersecurity of the organisation and ensuring its appropriate level. The main task of the team is to monitor and respond to potential threats in real time, as well as to maintain the protection of systems and data against cyber attacks. This team is is not kept informed of the details of ongoing testing, allowing simulations to be conducted in conditions as close to real-world conditions as possible. This allows to assess organisation's response to threats and test the effectiveness of existing procedures and defence mechanisms, thereby gaining a better understanding of the organisation's actual level of preparedness for incidents related to ICT.

Threat intelligence provider – is responsible for gathering information about threats to the organisation, using methods such as OSINT (open source intelligence). It collects intelligence data, analyses available public sources and other sources of information to create a comprehensive picture of the threats that may affect the organisation. TIP team is tasked with providing accurate and up-to-date information to help develop realistic scenarios for attacks carried out by RT. This ensures that the tests are better aligned with the threats that the organisation may face.

Red team – performs security tests in accordance with accepted and approved scenarios, using information, materials and data provided by TIP. The main task of RT is to simulate real attacks on organisation's systems in order to assess how effectively they can detect and respond to threats. Both technical and organisational security measures are tested. A holistic approach should enable the identification of potential weaknesses and gaps in the organisation's security. Red team uses various techniques and methods of attacks to make the tests as realistic and effective as possible. The reliability of the test results depends on the quality of the RT work. The higher the quality, the greater the chance of eliminating potential threats, mitigating identified risks and strengthening the level of security in the context of the functioning of the organisation.

Purple team – consists of members of RT and BT teams. The task of PT is to analyse the results obtained from the tests, identify areas for improvement and formulate recommendations that will help strengthen the organisation's security. Due to the cooperation of both teams, it is possible to more accurately assess the effectiveness of existing defence mechanisms and propose specific actions to improve both technical and procedural aspects of security.

TLPT implementation stages

Due to the complex and multifaceted nature of TLPT tests, they are carried out in three consecutive stages: preparation for testing, testing and summary. This approach increases the chances of conducting a reliable and in-depth assessment of the organisation's resilience to various types of threats.

In the first stage, i.e. the preparatory stage, the following activities are carried out:

- preliminary meetings between the entity conducting the tests and the supervisory authority and the TCT team to discuss and agree on the details of the tests, including the objectives, methodology and assessment criteria;

- defining the scope of the tests, i.e. the areas to be tested and potential threats to be considered. This step also involves setting the test objectives and expected results;
- procurement processes to select the appropriate RT and TIP teams. The selection of these teams is crucial to ensuring high-quality testing and realistic attack scenarios;
- preparing documentation specifying all aspects of the tests, including the schedule, communication rules, and safety procedures. This documentation provides the basis for subsequent testing stages and confirms that all parties agree on expectations and responsibilities.

The second stage during which the main testing activities are carried out includes:

- preparation of TTI (targeted threat intelligence) report and attack scenarios – TIP team provides a report regarding targeted TTI threats and preliminary attack scenarios. This report contains detailed information on potential threats and attack vectors that may affect organisation. On this basis TIP team creates realistic attack scenarios that will be used in further testing;
- RT conducts tests based on scenarios developed by TIP team, which allows for a thorough assessment of the resilience of the organisation's systems and procedures. Red team uses various techniques and methods of attacks to test how effectively the organisation deals with threats.

The third stage involves summarising and analysing the test results obtained, as well as developing recommendations. It consists of:

- preparation of reports by RT and BT teams. They include analyses of results, description of attack scenarios carried out, as well as assessment of the effectiveness of responses and defences. These documents are the basis for further analysis and conclusions regarding the organisation's security;
- conducting purple teaming workshops, during which RT and BT teams discuss past attack scenarios in order to exchange information and experiences. This allows for a better understanding of the effectiveness of the tests and identification of areas for improvement, as well as helping to develop practical recommendations and improvement plans;
- preparation of final report on the implementation of TLPT based on the reports from RT and BT teams as well as workshop results. It includes a summary of all activities carried out, conclusions from the tests, and recommendations for improving security. This document is submitted to the organisation and forms the basis for implementing security changes.

Summary and conclusions

As shown in the article, the basic premise of TLPT tests is to replicate real attacks as accurately as possible. This makes it possible to check not only the effectiveness of IT system security measures, but also the security level of operational processes and employee awareness of cyber threats, which increases the accuracy of assessing the resilience of organisation's systems and procedures. However, due to the complexity and diversity of TLPT tests, their implementation may pose a challenge for organisation. They require careful preparation and appropriate procedures to ensure both the effectiveness of the tests and the safety of the organisation during their implementation.

The analysis conducted for the purposes of this article leads to the conclusion that the implementation of TLPT tests as a standard for financial entities was a step in the right direction. There is no doubt that in a complex digital environment, it is necessary to develop effective risk management mechanisms based on real factors and challenges, and not only those defined for the purposes of building appropriate models. The authors share the position of the European Central Bank, which emphasises that TLPT tests allow for the verification not only of technical means, but also of personnel and processes. This bank rightly points out that (…) *the results of these tests can significantly increase the security awareness of the senior management within the entities being tested*[27]. Wojciech Dworakowski is also right when he points out that TLPT is an investment in security that pays off, because it is better to be proactive than to repair the damage caused by a cyberattack[28].

In the coming years, it will be crucial to ensure consistent and proportionate application of TLPT tests across the EU financial sector. Financial supervision should take advantage of this opportunity to support entities in preparing for these tests and in developing their capabilities to defend themselves against cyber attacks. Verifying the organisation's resistance using realistic attack scenarios should significantly contribute to improving the cyber resilience of the entire financial market.

---

[27] *Opinion of the European Central Bank of 4 June 2021 on a proposal for a regulation of the European Parliament and of the Council on digital operational resilience for the financial sector (CON/2021/20)*, p. 1.

[28] W. Dworakowski, *Threat-Led Penetration Testing (TLPT) – Jak być zgodnym z DORA w 2025 roku?* (Eng. Threat-Led Penetration Testing (TLPT) – How to be DORA compliant in 2025?), Securing, 28 II 2025, https://www.securing.pl/en/threat-led-penetration-testing-tlpt-how-to-be-dora-compliant-in-2025/ [accessed: 18 IV 2025].

Bibliography

Bayle de Jessé M., *The Eurosystem's cyber resilience strategy for financial market infrastructures*, "Cyber Security: A Peer-Reviewed Journal" 2019, vol. 2, no. 4, pp. 294–302. https://doi.org/10.69554/DFBJ2963.

Cichocki C., Komentarz do art. 26 (Eng. Commentary on Article 26), in: *Rozporządzenie UE w sprawie operacyjnej odporności cyfrowej sektora finansowego (DORA). Komentarz*, J. Byrski, J. Kurek-Sobieraj (eds.), Warszawa 2025, pp. 276–282.

Cichocki C., Komentarz do art. 27 (Eng. Commentary on Article 27), in: *Rozporządzenie UE w sprawie operacyjnej odporności cyfrowej sektora finansowego (DORA). Komentarz*, J. Byrski, J. Kurek-Sobieraj (eds.), Warszawa 2025, pp. 283–286.

Dozsa M.L., *Modular Automated Cyber Range Deployment with Adversary Emulation. In Compliance with the Digital Operational Resilience Act (DORA)*, master's thesis, Oslo 2024.

Kurek-Sobieraj J., Komentarz do art. 3 (Eng. Commentary on Article 3), in: *Rozporządzenie UE w sprawie operacyjnej odporności cyfrowej sektora finansowego (DORA). Komentarz*, J. Byrski, J. Kurek-Sobieraj (eds.), Warszawa 2025, pp. 69–106.

Riaz B., Younas Z., *Investigating the impact of DORA Regulations on Third Party Risk Management in the Swedish Financial Sector*, Stockholm University 2024.

Scott B.F., *Red teaming financial crime risks in the banking sector*, "Journal of Financial Crime" 2021, vol. 28, no. 1, pp. 98–111. https://doi.org/10.1108/JFC-06-2020-0118.

Valkeasuo T., *TIBER-EU Preparation Phase Framework Case study Nixu: optimizing TIBER-EU engagements*, Jyväskylä: JAMK University of Applied Sciences, March 2023.

Internet sources

Dworakowski W., *Threat-Led Penetration Testing (TLPT) – How to be DORA compliant in 2025?*, Securing, 28 II 2025, https://www.securing.pl/en/threat-led-penetration-testing-tlpt--how-to-be-dora-compliant-in-2025/ [accessed: 18 IV 2025].

Implementacje frameworku TIBER-EU w Europie a wdrożenie w Polsce (Eng. Implementations of the TIBER-EU framework in Europe and implementation in Poland), Komisja Nadzoru Finansowego, 27 I 2025, https://www.knf.gov.pl/?articleId=91971&p_id=18 [accessed: 19 IV 2025].

Krajobraz cyberzagrożeń w polskim sektorze finansowym 2025 (Eng. The cyber threat landscape in the Polish financial sector 2025), CSIRT KNF, https://cebrf.knf.gov.pl/images/GTL_2025_FINAL.pdf [accessed: 19 I 2026].

Testy TLPT – cyfrowa odporność organizacji zgodnie z rozporządzeniem DORA (Eng. TLPT tests – digital resilience of organisations in accordance with the DORA regulation), Bankowe ABC, 2 I 2025, https://bankoweabc.pl/2025/01/02/testy-tlpt-a-dora/ [accessed: 19 IV 2025].

Testy TLPT – nowe podejście do testowania cyfrowej odporności organizacji (Eng. TLPT tests – a new approach to testing the digital resilience of organisation), Komisja Nadzoru Finansowego, 14 VII 2025, https://www.knf.gov.pl/dla_rynku/dora/wymagania_rozporzadzenia_dora/testy_TLPT_nowe_podejscie?articleId=90547&p_id=18 [accessed: 9 II 2026].

TIBER-EU Framework. How to implement the European framework for Threat Intelligence-Based Ethical Red teaming, European Central Bank, January 2025, https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework_2025~b32eff9a10.pl.pdf?0309990e5e167a47ca4748370a949064 [accessed: 9 II 2026].

TIBER-EU Guidance for Service Provider Procurement, European Central Bank, January 2025, https://www.ecb.europa.eu/pub/pdf/annex/ecb.tiber_eu_service_provider_procurement_2025.en.pdf?1d229f2191835b83770d593a44f69b14 [accessed: 19 IV 2025].

TIBER-EU i DORA szansą na budowanie realnej cyberodporności w sektorze finansowym (Eng. TIBER-EU and DORA as an opportunity to build real cyber resilience in the financial sector), Z-LABS, 8 VII 2024, https://blog.z-labs.eu/2024/07/08/tiber-eu-dora-cyberodpornosc.html [accessed: 19 IV 2025].

TIBER-EU Purple Teaming Guidance, European Central Bank, January 2025, https://www.ecb.europa.eu/pub/pdf/annex/ecb.tiber_eu_purple_best_practices_2025.en.pdf?759d46ff75caf6e644af0fd757415aee [accessed: 19 IV 2025].

TIBER-EU Scope Specification Document Guidance, European Central Bank, January 2025, https://www.ecb.europa.eu/pub/pdf/annex/ecb.tiber_scope_specification_document_guidance_2025.en.pdf?67dc9f94d617ea2522e9a3764f43b92c [accessed: 19 IV 2025].

TIBER-EU Test Summary Report Guidance, European Central Bank, January 2025, https://www.ecb.europa.eu/pub/pdf/annex/ecb.tiber_test_summary_report_guidance_2025.en.pdf?ecc819840c37a008b908578dd1d48b50 [accessed: 19 IV 2025].

Ustawa wdrażająca DORA do prawa polskiego (Eng. Act implementing DORA into Polish law), "Biuletyn prawny dla branży finansowej", Deloitte, https://www.deloitte.com/pl/pl/Industries/financial-services/perspectives/ustawa-wdrazajaca-DORA-do-prawa-polskiego.html [accessed: 12 IV 2025].

Legal acts

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 (Official Journal of the EU L 333 of 2022, as amended).

Council Regulation (EU) No 1024/2013 of 15 October 2013 conferring specific tasks on the European Central Bank concerning policies relating to the prudential supervision of credit institutions (Official Journal of the EU L 287 of 2013).

Act of 25 June 2025 on amendments to certain acts in connection with ensuring the operational digital resilience of the financial sector and the issuance of European green bonds (Journal of Laws of 2025, item 1069).

Act of 21 July 2006 on financial market supervision (consolidated text, Journal of Laws of 2025, item 640, as amended).

Other documents

Final Report. Draft Regulatory Technical Standards specifying elements related to threat led penetration tests under Article 26(11) of Regulation (EU) 2022/2554, European Banking Authority, 17 July 2024.

Opinion of the European Central Bank of 4 June 2021 on a proposal for a regulation of the European Parliament and of the Council on digital operational resilience for the financial sector (CON/2021/20) – (Official Journal of the EU C 343/1 of 2021).

Draft law amending certain laws in connection with ensuring the operational digital resilience of the financial sector and the issuance of European Green Bonds, print no. UC11, Rządowe Centrum Legislacji, Warszawa 2025.

Assoc. Prof. Kamil Mroczka

Post-doctoral degree in social sciences in the field of political science and administration, assistant professor in the Department of State and Public Administration at the Faculty of Political Science and International Studies of the University of Warsaw, graduate of the Executive MBA programme. He has many years of experience in managerial positions in public administration and in the private sector. He is currently employed as Chief Compliance Officer at Santander Bank Poland.

Contact: ks.mroczka@uw.edu.pl

Paweł Piekutowski

Graduate of the Military University of Technology in Warsaw. He has many years of professional experience in the field of cybersecurity, particularly in the area of penetration testing. He currently serves as Deputy Director of the Cybersecurity Department at the Polish Financial Supervision Authority (UKNF).

Contact: pawel.piekutowski@gmail.com