EUROPEAN CENTRAL BANK

BANKING SUPERVISION

TIBER-EU SSM Implementation Guide

How to implement the TIBER-EU framework for the DORA TLPT of significant institutions

Executive summary

Under Articles 26 and 27 of the Digital Operational Resilience Act (DORA)[1], identified financial entities must carry out, at least every three years[2], advanced operational resilience testing by means of threat-led penetration testing (TLPT). The European Central Bank (ECB) is the competent authority (CA) and TLPT authority (TLPTA) for significant institutions (SIs)[3] under Articles 26 and 46 DORA and is thus ultimately responsible for the operationalisation of TLPT. To help SIs fulfil the DORA TLPT requirements, the ECB has decided to adopt the Framework for Threat Intelligence-based Ethical Red Teaming (TIBER-EU)[4].

The aim of a correctly performed TLPT is to provide a learning experience for the SI and to serve as an effective supervisory tool. The TIBER-EU framework enables European and national authorities to perform TLPT for financial entities within their remit in order to further strengthen these entities' resilience to sophisticated cyberattacks.

This guide sets out how the ECB adopts and implements the TIBER-EU framework for the TLPT of SIs as identified for TLPT according to DORA. This means that, for any SI identified by the ECB as falling under the DORA requirement to undergo mandatory TLPT, this document can be used as guidance on how to fulfil the requirements under DORA and the accompanying Regulatory Technical Standards (RTS) on TLPT[5]. Note that only the requirements under DORA and the RTS are legally binding, and they take precedence over the TIBER-EU framework.

---

1 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 (OJ L 333, 27.12.2022, p. 1). DORA has been applicable since 17 January 2025 and provides for threat-led penetration testing of financial entities identified in accordance with Article 26(8).

2 The ECB may alter the frequency of tests under Article 26(1) DORA.

3 Institutions identified by the ECB as "significant" under the SSM Regulation 1024/2013.

4 See "TIBER-EU framework: How to implement the European framework for Threat Intelligence-Based Ethical Red Teaming".

5 The RTS on TLPT are set out in Commission Delegated Regulation (EU) 2025/1190 of 13 February 2025 supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying the criteria used for identifying financial entities required to perform threat-led penetration testing, the requirements and standards governing the use of internal testers, the requirements in relation to the scope, testing methodology and approach for each phase of the testing, results, closure and remediation stages and the type of supervisory and other relevant cooperation needed for the implementation of TLPT and for the facilitation of mutual recognition (OJ L 333, 27.12.2022, p. 1).

1 Introduction

Threat intelligence-based ethical red teaming (TIBER-EU) is a common framework in the European Union (EU) established by the ECB that delivers controlled, bespoke, intelligence-led red team tests[6] of entities' critical live production systems. As such, it harmonises the varying practices adopted by different entities when conducting red teaming. This harmonisation ensures that red team testing is of high quality and is universally accepted EU-wide. It also enables multi-jurisdictional testing to be conducted throughout the EU. The ECB published the TIBER-EU framework in May 2018, with an update in January 2025[7]. Since then, the framework has been adopted and implemented by EU and national authorities. Additional guidance and templates have been published on a dedicated page of the ECB's website[8].

The EU adopted the Digital Operational Resilience Act (DORA)[9] in December 2022. Among other things, DORA provides for threat-led penetration testing (TLPT)[10] to be carried out on financial entities identified by their respective competent authorities (CAs). Regulatory Technical Standards (RTS) on TLPT were issued on 18 June 2025 on the basis of Article 26(11) DORA. The RTS on TLPT require significant institutions (SIs) designated as global systemically important banks (G-SIBs) and other systemically important institutions (O-SIIs), as well as parts of such institutions[11], to undergo TLPT. The ECB may define additional criteria to further limit or extend the number of SIs required to undergo TLPT and/or the frequency of TLPT.

1.1 How does TIBER-EU relate to DORA TLPT?

To avoid fragmentation in the approach to TLPT within the European Union and to ensure a level playing field, the legislators required the RTS on TLPT to be drafted "in accordance with the TIBER-EU framework" (Article 26(11) DORA). DORA and the RTS on TLPT set out precise but high-level legal requirements on what needs to be done or achieved during a test (the "what"). The TIBER-EU framework (including its various implementations) is a detailed, non-legally binding explanation and operationalisation of how TLPT should be conducted, both by the tested entities and

6 Intelligence-led red-team tests mimic the tactics, techniques, and procedures (TTPs) of real-life threat actors who, on the basis of threat intelligence, are perceived as posing a genuine threat. An intelligence-led red team test involves the use of various techniques to simulate a cyberattack on an entity's critical or important functions (CIFs) and underlying systems (i.e. its people, processes and technologies). It helps the entity to assess its protection, detection and response capabilities.

7 See "TIBER-EU framework: How to implement the European framework for Threat Intelligence-based Ethical Red Teaming", January 2025.

8 See "What is TIBER-EU?" on the ECB's website for guidance and templates.

9 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 (OJ L 333, 27.12.2022, p. 1). DORA has been applicable since 17 January 2025 and provides for threat-led penetration testing of financial entities identified in accordance with Article 26(8) of DORA.

10 Also referred to as "advanced digital operational resilience testing".

11 For example, but not limited to, parent undertakings and subsidiaries.

by the TLPTA that has chosen to adopt it (the “how”). The ECB has also published a paper explaining the precise relationship between DORA TLPT and TIBER-EU[12].

1.2 What is the purpose of this guide?

This guide describes how the TIBER-EU framework is adopted and implemented by the ECB for the mandatory DORA TLPT of the SIs[13] as identified by the ECB. It provides guidance to SIs and all relevant stakeholders on the approach to be taken when carrying out the TLPT in practice, with the aim of helping fulfil the requirements under DORA and the RTS on TLPT, while at the same time offering flexibility to adapt each test to the specific characteristics of the individual SI. The guide should thus be viewed as an implementation of TIBER-EU and is designed to be consistent with similar implementations by other authorities (TIBER-DE, TIBER-ES, etc.) and not as a separate framework adjacent to, or superseding, the TIBER-EU framework itself. Against this backdrop, this guide aims to provide a common understanding for the DORA TLPT of SIs.

1.3 Relationship of TIBER-EU SSM to other TIBER authorities

The implementation of TIBER-EU for the Single Supervisory Mechanism (TIBER-EU SSM) is concerned only with the TLPT of SIs under DORA; there are other implementations of TIBER-EU by CAs and TLPTAs at national and European level. Through the TIBER-EU SSM implementation, the ECB aims to cooperate with the relevant authorities on TLPT matters and minimise differences between TLPT approaches while allowing for cooperation where relevant.

If an SI (or subsidiary) opts to undergo a voluntary TIBER test following DORA becoming applicable on 17 January 2025 (e.g. as part of its digital operational resilience testing programme), the ECB as TLPTA will be informed, and any voluntary test can be performed for an SI via the relevant national TLPT cyber team (TCT), provided it has adopted the TIBER-EU framework and has its own implementation. In such a case, given that the test is conducted on a voluntary basis, it will not be considered a DORA TLPT and will not be taken into account for the timing of the SI’s mandatory DORA TLPT.

2 TIBER-EU SSM implementation

TLPT conducted for SIs will utilise the TIBER-EU framework process, which helps entities and authorities fulfil the requirements of DORA and the RTS on TLPT.

A TLPT authority (TLPTA) is any authority tasked under DORA with conducting one or more regulatory tasks as part of TLPT. Since TIBER-EU is used as a means of

12 See “Adopting TIBER-EU will help fulfil DORA requirements”.

13 SIs and, where applicable, subsidiaries/parent entities that are also credit institutions.

conducting the TLPT of identified SIs under DORA, for the purpose of this guide the term “TIBER authority” used in the TIBER-EU framework is interchangeable with the term “TLPT authority”. Similarly, the term “TLPT Cyber Team” is interchangeable with the term “TIBER Cyber Team” and “TIBER-EU SSM test” is interchangeable with “DORA TLPT”. In the context of DORA TLPT of SIs, the ECB is the TLPTA for identified SIs and is ultimately responsible for all aspects of TLPT.

The ECB as TLPTA identifies the SIs that are to undergo mandatory TLPT based on the provisions of DORA and the RTS on TLPT. Additionally, the ECB establishes an SSM TLPT cyber team (TCT-SSM) responsible for all related TLPT activities assigned to it.[14]

In its capacity as TLPTA, the ECB may make use of the national TCTs for the monitoring and oversight of the TLPT of SIs. The ECB will assign such TLPT either to the TCT-SSM or to a national TCT (located at a national competent authority and/or national central bank). In all cases the test should be performed according to the guidance in this document to help fulfil the requirements of DORA and the RTS on TLPT.

2.1 Identified SIs

The ECB must identify SIs that are subject to mandatory TLPT under Article 26(8) DORA and Article 2 of the RTS on TLPT. It uses criteria relating to systemic importance, business impact and ICT risk profile in line with current practices in place within the SSM. A list of identified entities will be maintained by the ECB, with annual updates or adjustments as needed.

The ECB will inform the relevant SIs that they have been identified as subject to mandatory TLPT. It will require each of the SIs identified to appoint a single point of contact (SPOC) for each test to ensure secrecy. The SPOC should have sufficient authority along with knowledge of the entity’s IT systems and business processes15. Once the test begins, this person should be included in the control team (CT). The SPOC may receive relevant information on TLPT from the TLPTA. It is the responsibility of the SI to inform the ECB and relevant TCT without undue delay if the contact details of the SPOC change or a new SPOC is appointed.

2.2 TIBER-EU SSM contact information

The TCT-SSM can be contacted at TCT-SSM@ecb.europa.eu for any queries relating to TLPT of SIs. General questions regarding the TIBER-EU framework should be directed to TIBER-EU@ecb.europa.eu.

---

[14] The SSM TLPT Cyber Team (TCT-SSM) comprises staff within the ECB that are responsible for all matters related to TLPT.

[15] Usually these would be individuals in the roles of, or reporting directly or indirectly to, the Chief Information Security Officer, Chief Risk Officer, Chief Technology Officer and/or Chief Information Officer.

3 Key stakeholders involved in TIBER-EU SSM

A DORA TLPT of an SI requires the involvement of different stakeholders who have clearly defined roles and responsibilities and are bound by secrecy. All main stakeholders involved in a DORA TLPT should be fully informed about their respective roles and responsibilities to ensure that they can perform any actions relating to their role. The involvement of stakeholders in this way is necessary for the test to be conducted in a safe and controlled manner.

A test on an SI specifically requires the involvement of the following stakeholders:

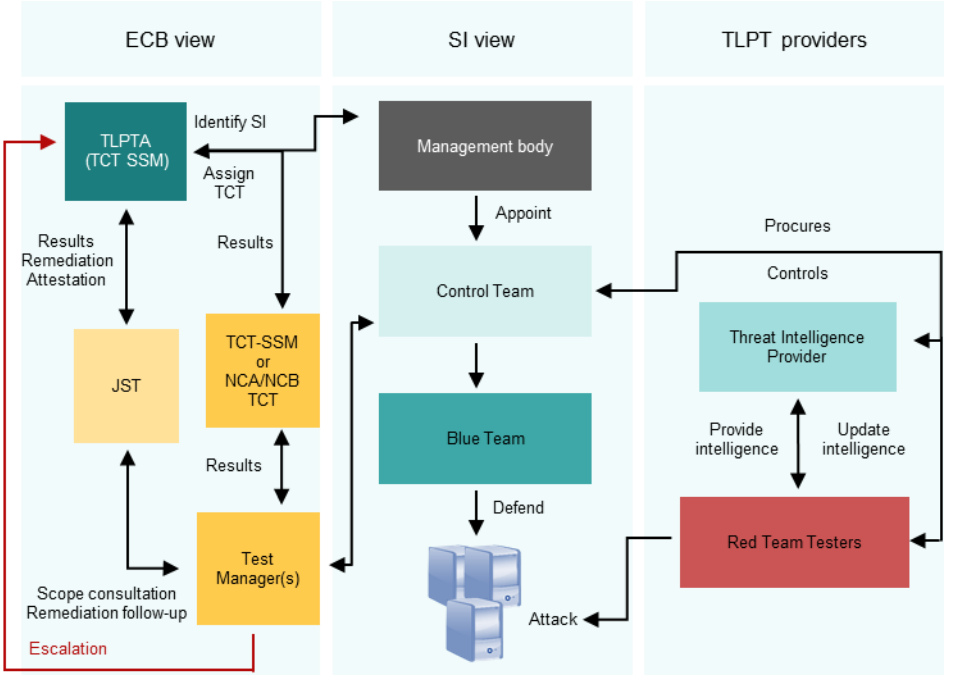
- the ECB as TLPT authority (TLPTA);
- the TLPT cyber team (TCT) and test managers (TMs);
- the SI's management body;
- the Control Team (CT) and Control Team Lead (CTL) in the SI;
- the Threat Intelligence Provider (TIP);
- Red Team Testers (RTT);
- one or more ICT service providers (ISPs) if included in the scope of the TLPT;
- a Blue Team (BT), which is unaware of the test being conducted[16];
- the Joint Supervisory Team (JST) that supervises the bank.

The stakeholder roles are outlined at a high level in the figure below and described in more detail in the following sections[17]. All stakeholders should work closely together in a spirit of trust and cooperation. This reflects the objective of the test, which is not simply to indicate whether or not an SI meets the requirements, but also, if performed properly, to provide the SI with an insight into its strengths and weaknesses, enabling it to learn and achieve a higher level of cyber maturity.

[16] Unless the CT informs the BT after receiving the TM's approval to do so.

[17] More details on the stakeholders can be found in the "TIBER-EU Framework".

Figure 1
TLPT stakeholder roles



3.1 TLPT authority

For SIs, the ECB will perform the functions of the TLPT authority under DORA. These activities are operationalised by the TCT-SSM that is located in the Directorate General On-site and Internal Model Inspections (DG/OMI).

The TCT-SSM will identify SIs subject to TLPT by applying the legal requirements. SIs that have been identified will receive relevant communication informing them that they are subject to TLPT.

For each identified SI, a test will be structured into a single entity or joint test. Subsequently, the ECB will assign each test to a responsible TCT, also appointing the TMs responsible for the oversight of the TLPT. In case of an emergency or serious issue during the TLPT, the TCT-SSM must be notified by the appointed TM. Following the conclusion of any TLPT that fulfils the requirements of DORA and the RTS on TLPT, the TCT-SSM is responsible for organising the issuance of an attestation.

The TCT-SSM will also maintain contact with the relevant Joint Supervisory Teams, the national TCTs and other authorities for TLPT purposes.

3.2 TLPT Cyber Team and Test Managers

The TLPT Cyber Team (TCT) assigned to each test is tasked with all operational matters and actions related to carrying out the actual test. The TCT, assigned by the ECB as TLPTA, will assume responsibility for the test on its behalf. Any tests assigned to national TCTs will be scheduled together with the TCT-SSM.

The TLPTA will appoint a dedicated Test Manager (TM) and at least one alternate TM to each DORA TLPT. The role of the TM is to make sure that the SI undergoes the test in a uniform and controlled manner, and in accordance with this guide.

The TM is independent from the CT and is not accountable for the CT's actions, the running of the test, or the results or the remediation planning. In the case of certain tests (e.g. joint tests) TMs from multiple relevant TLPTAs may take part or act as observers.

During a DORA TLPT, the TM will assess whether the SI is conducting the test in accordance with DORA and the RTS on TLPT. The TM will inform the CTL if a risk of non-compliance emerges, to allow for corrective action to be taken. If the situation is not remedied then the TM will inform the TCT-SSM without undue delay. The TCT-SSM may take further action, including further escalation, ending the test and requiring it to be repeated, or any other course of action the ECB deems appropriate. In exceptional cases, where the requirements are not met, the TLPTA may decide not to issue an attestation. In such a situation the SI can choose to continue the test, to gain insights and enhance its learning experience, without the test being recognised as a DORA TLPT.

3.3 Management body of the SI

The management body of the SI is accountable for the safe and proper conduct of the DORA TLPT. It is also responsible for approving the scope of the test. It may delegate responsibility for managing the test, including procuring the threat intelligence and red team provider, to the CTL.

3.4 Control Team and Control Team Lead

For each DORA TLPT, the RTS on TLPT requires the SI undergoing the test to form a Control Team (CT) and appoint a Control Team Lead (CTL) to manage the test. The CT is responsible for the overall planning and management of the test and plays a central role in the testing process, coordinating all test activity. The CTL should ensure that the TIP's and RTT's project plans are factored into the SI's overall project planning for the DORA TLPT. One or more members of the CT should be positioned in such a manner that they will know and have access to any detection by the BT or ISP. The TM is closely involved in the test and in liaising with the CTL to ensure that the test proceeds according to the applicable process, milestones and deliverables. The aim is to maximise the learning experience while minimising the

risk for the SI. More information on the composition of the CT can be found in the TIBER-EU Control Team Guidance.[18]

3.5 Blue Team

For each DORA TLPT, there is a Blue Team (BT) made up of staff from the SI, (the SI's ISP) and any other party deemed relevant considering the scope of the test. The BT is not part of the CT and is not aware of the test being carried out. More specifically, the BT defends the SI's use of network and information systems by maintaining its security posture against simulated or real attacks. It is of critical importance for the BT to be unaware of both the preparation and conduct of the DORA TLPT unless the CT, subject to the agreement of the TM, informs the BT. The BT drafts the Blue Team Test Report (BTTR) during the closure phase of the TLPT.

3.6 Threat Intelligence Provider

The TIP[19] provides threat intelligence (TI) to the SI in the form of a Targeted Threat Intelligence Report (TTIR), which can be further enhanced by the Red Team Testers (RTT) through cooperative active TI. The TTIR sets out the threat scenarios, and the TIP works with the RTT to develop these into attack scenarios. The TIP is also invited to provide input into the final Red Team Test Report (RTTR) issued to the SI. The TIP should cooperate with the RTT during the DORA TLPT. In addition to developing attack scenarios with the RTT, this includes working together on any new intelligence requirements that arise as the red team test progresses.

Under Article 27 DORA, the TIP should be external to an SI undergoing TLPT.

3.7 Red Team Testers

The Red Team Testers (RTTs)[20] aim to assess the cyber defences of an SI by executing the red team scenarios documented in the Red Team Test Plan (RTTP). These scenarios are in turn developed from the TI Provider scenarios. The RTTs should follow a rigorous and ethical red team testing methodology and should meet the minimum requirements defined under the TIBER-EU framework. The rules of engagement and specific testing requirements should be established by the RTTs and the CT. The RTTs are expected to work closely with the TIP, which includes reviewing and commenting on the intelligence deliverables (once approved by the TM) as well as transforming threat scenarios into cohesive and tractable test scenarios in the RTTP. The RTTs are expected to liaise and work with the TIP throughout the testing to update the threat intelligence assessment and attack

[18] See "TIBER-EU Control Team Guidance".

[19] See "TIBER-EU Guidance for Service Provider Procurement" for more details on the qualifications and certifications needed by threat intelligence providers, along with other requirements.

[20] See "TIBER-EU Guidance for Service Provider Procurement" for more details on the qualifications and certifications needed by threat red team testers, along with other requirements.

scenarios with relevant and up-to-date intelligence. The RTT drafts an RTTR that includes issues identified during the test.

Under Article 26(8) DORA, only external RTTs[21] must be used for the TLPT of SIs.

3.8 ICT service provider

An SI may be supported by one or more ICT service providers (ISPs) for the ICT systems underpinning its critical or important functions (CIFs) that are in the scope of the TLPT. The ISP may be either intragroup or a third party. Its responsibilities may include, but are not limited to, the provision, administration and support of ICT services or infrastructure. As such, the infrastructure, processes and people relevant to the SI's systems within the scope of the TLPT and located at the ISP(s) should be considered for inclusion in the scope of the test depending on the services in question and the extent to which they support or can adversely affect these systems.

Depending on the nature of the service and/or the level of dependence of the SI on the ISP and the contractual arrangement, the involvement of the ISP during the test may differ, for example depending on whether a representative from the ISP needs to join the CT. This involvement will be determined during the preparation phase, and the SI should be prepared for such a situation beforehand.

4 The TIBER-EU SSM testing process

Before the start of the DORA TLPT, the ECB will identify the SIs that are subject to the DORA requirement to undergo mandatory TLPT and inform the SIs identified. The SIs are expected to appoint a SPOC with adequate knowledge and authority to communicate and liaise with the TCT-SSM, and any national TCT assigned, on TLPT matters. SIs are also expected to inform the TLPTA of the SPOC's identity. The SPOC is expected to be a member of the CT once the test begins.

The TIBER-EU SSM process consists of three mandatory phases: (i) preparation, (ii) testing, and (iii) closure.

4.1 Preparation

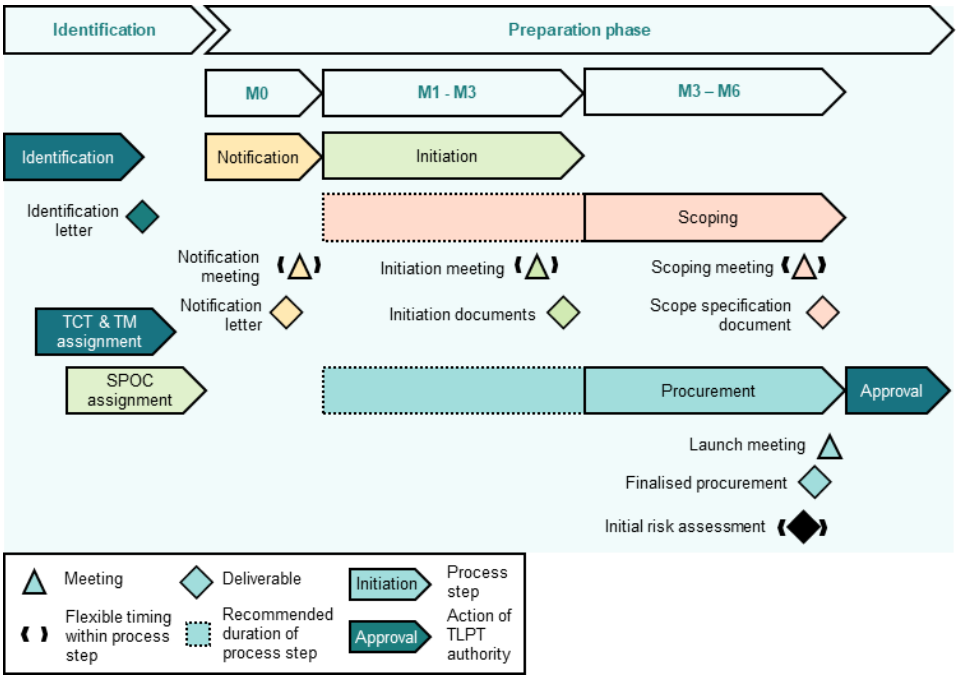
The preparation phase of a DORA TLPT starts when the SI's designated SPOC receives a notification letter from the TLPTA (ECB) giving details of the TM responsible for the test. The TM appointed to the test then starts liaising with the SI. The SI selects a CTL, forms a CT and drafts the initiation documents, which include a high-level project plan as well as communication details. The SI completes an initial risk assessment and takes appropriate measures to mitigate the risks identified. The scope is defined in a dedicated document, and the SI procures the

[21] DORA refers simply to "red teams", while TIBER-EU uses the term "Red Team Testers" and the abbreviation "RTT".

TIP and RTT. The TM validates the initiation documents and CT composition, as well as approving the scope specification document. The TM is consulted on the risk assessment by the CT before the testing phase.

The figure below shows the process for the preparation phase, including all milestones, meetings and deliverables.

Figure 2
Preparation phase (M[X] refers to the duration of months)



4.2 Testing

The testing phase is divided into the threat intelligence sub-phase and the red-teaming sub-phase.

The process for the threat intelligence sub-phase consists of two steps: (i) TI collection and scenario creation, and (ii) TTI report creation.

In the first of these two steps, the TIP collects, analyses and disseminates tailored intelligence relating to two key areas of interest:

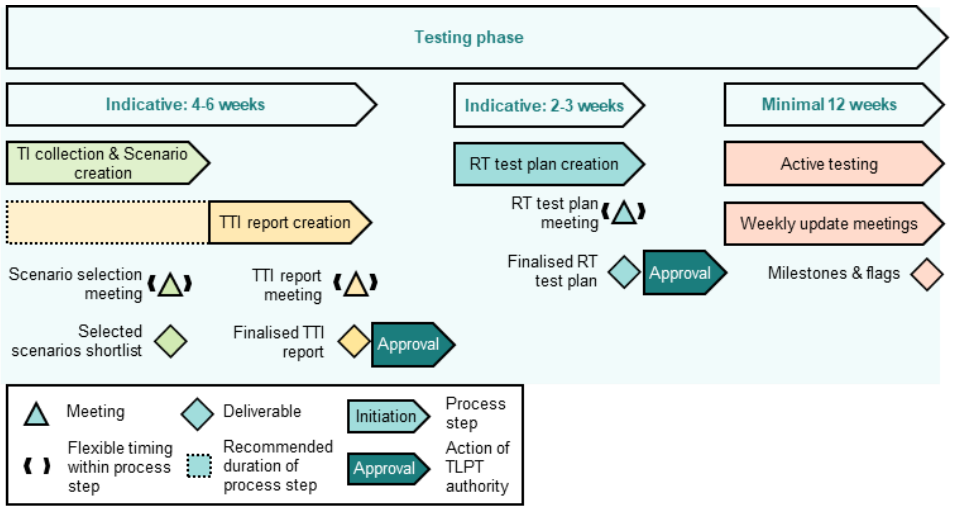
1. Target intelligence or information on potential attack surfaces and exposures across the SI.

2. Threat intelligence or information on relevant threat actors and probable threat scenarios. Based on this information the TIP should develop a broad set of high-level scenarios tailored to the SI undergoing the test and from which test scenarios will be selected.

Additionally, the TIP should draft a dedicated TTIR outlining the tailored threat landscape and elaborating further on the scenarios. When the TTIR is in its final stage, a TTIR meeting should be held to discuss the reported findings. Once approved by the TM, the TTIR should form the basis for the RTTP creation in the red-teaming subphase.

The red teaming sub-phase is where the RTTs plan and execute a DORA TLPT on the basis of the selected scenarios for the target systems that underpin the selected CIFs in scope. The process for the testing phase consists of two separate steps: (i) RTTP creation, and (ii) active testing. The figure below shows the process for the testing phase, including all milestones, meetings and deliverables.

Figure 3
Testing phase



4.3 Closure

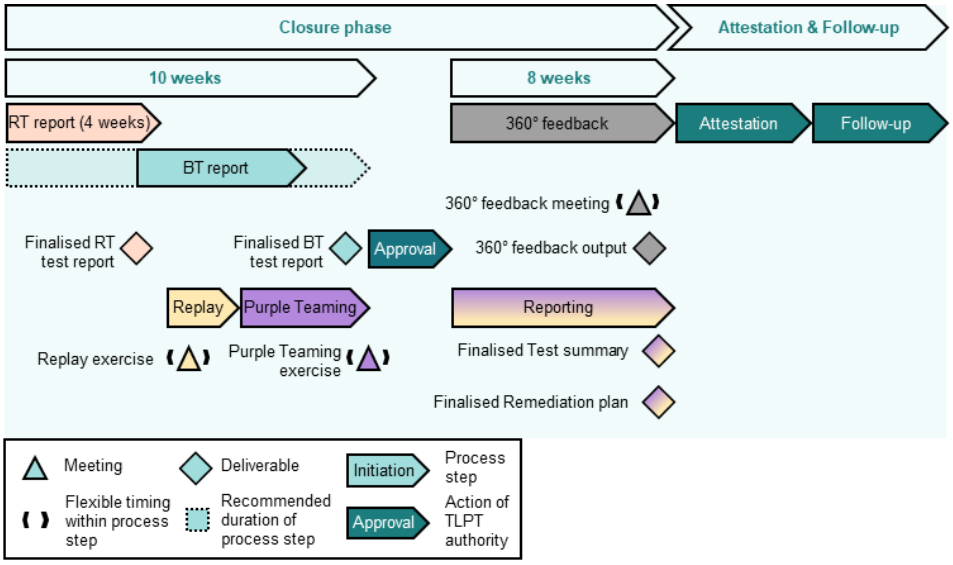
The closure phase allows all relevant stakeholders to reflect on the results of the test and make improvements to further enhance the cyber resilience of the SI. Once the active testing is concluded and the BT has been informed about the test, the RTT and the BT should begin drafting their respective test reports. The RT Test Report (RTTR) includes details of the approach taken to the testing and the findings and observations from the test, whereas the BT Test Report (BTTR) should include details on the team's observations during the test, mapped alongside the actions of the RTT. The BT may use the RTTR as the basis for its BTTR.

Once these reports have been checked by the TM, the replay[22] and Purple-Teaming exercises should be conducted. After the replay and Purple-Teaming, the CT should finalise the Test Summary Report (TSR) and remediation plan. A 360-degree

[22] Replay means the replay exercise covering the offensive and defensive actions that takes place after the end of the active red team testing phase. It is a necessary step in the process and is included in the RTS on TLPT and the TIBER-EU framework.

feedback round should then be held, in which all relevant stakeholders deliver feedback to each other and on the overall testing process. The closure phase should be completed with the finalisation of the TSR (to be approved by the TM) and remediation plan. Following the end of the testing process, the JST will assess the results and remediation plan. The culmination of a TLPT is the attestation, issued by the TLPTA, that the test has been conducted in accordance with the requirements of DORA and the RTS on TLPT. If an attestation cannot be provided, the SI will be formally informed by the TLPTA of this and potential next steps. The figure below shows the process for the closure phase, including all milestones, meetings and deliverables.

Figure 4
Closure phase



5 General considerations for TLPT

5.1 Test management

The CT has ultimate, end-to-end responsibility for the conduct of the TLPT in their own SI and should therefore remain in control of the process. The TM should be closely involved in the test to ensure that it proceeds according to the process, milestones and deliverables as agreed and described in this implementation guide and further in the TIBER-EU framework and accompanying guidance. The aim is to maximise the learning experience while minimising the risk for the SI.

5.2 Procurement and contracting

The CT is responsible for procuring competent, qualified TI and RTT providers with the required experience and skills to conduct the tests based on the TIBER-EU Guidance for Service Provider Procurement and in line with the procurement rules and regulations. SIs can only use external TI providers and RTT in accordance with Article 26(8) DORA. The CT arranges and budgets for procurement. However, the CT should not proceed with contracting the selected TIP and external RTT if the TM is of the opinion that the selected TIP and external RTT do not ensure compliance with the requirements under Article 7(1) RTS on TLPT.

The CT should make sure, when formally contracting TI and RT providers for their SI, that there is mutual agreement on at least the following aspects:

- the infrastructure in scope of the test and its boundaries;
- the confidentiality of the test and the information provided or obtained;
- the timing and availability of the providers;
- the actions forbidden during testing, such as uncontrolled modification of data or programs, jeopardising the continuity of critical services, blackmail, harming, threatening or bribing employees, disclosure of results, etc.;
- secure communication channels;
- the alerting and escalation procedures;
- liability (including insurance);
- the languages required for communication during the test.

In addition to these elements, the contracts with the TI and RTT providers should ensure that, among other things:

- the providers are able to ensure the availability of testers with the required skillset, including, for example, in the event of staff rotation or delays to the test;
- the providers have adequate governance, security and risk management measures in place, including data retention, protection and destruction requirements and breach notification provisions;
- the providers can cater for the particularities of a test, for example with regard to the languages spoken or the jurisdictional set-up of the test;
- the absence of any conflict of interest on the part of the procured provider.

The TIBER-EU Guidance for Service Provider Procurement sets out in further detail the operational aspects for the SI and TI/RTT providers to consider when formalising their contractual arrangements.

5.3 Secrecy

Protecting and ensuring the secrecy and confidentiality of the test is crucial to its effectiveness. To that end, only a small and trusted group, namely the CT and relevant members of the management body, should be aware of the test. The CT should include member(s) that have the appropriate levels of seniority to make risk-based decisions regarding the test.

It is up to the SI's CT to appropriately safeguard the information created and owned by the CT during and after the test. The TIP/RTT should include appropriate clauses and commitments to maintaining confidentiality and secrecy with regard to TLPT and any information divulged during the test.

If, during the testing process, the CT suspects that secrecy has been breached, for example if the BT is aware of the test taking place and could therefore act in such a way as to undermine its integrity, it should inform the TM immediately. Upon realising or being informed that the secrecy of the test has been breached, the TM will escalate the matter to the TLPTA and/or consider the conditions for issuing an attestation as not being met.

5.4 Communication

Communication among the different stakeholders is essential during the DORA TLPT. Communication should be conducted via secure communication channels to ensure that the test remains secret. These channels should be discussed with the TM and agreed upon during the preparation phase. Communications with external parties such as the TIP and RTT should be agreed upon before these parties begin to provide services. The CT and TM should be in constant communication with each other throughout the process. With regard to the test, the TM is the primary contact for the CT.

5.5 Risk management

By construction, the DORA TLPT carries elements of risk for all parties owing to the criticality of the SI undergoing the test. The possibility of causing a denial-of-service incident, an unexpected system crash, damage to critical live production systems, or the loss, modification or disclosure of data highlights the need for active and robust risk management.

The CT should conduct a risk assessment before the test takes place. Throughout the TLPT process, the CT should ensure that it gives due consideration to the risks associated with the test, both before and during the test. To reduce the risks associated with testing, sufficient planning and coordination should take place before and during the test. The CT should share the pre-test risk assessment with the TM for review before the testing phase. If the assessment changes significantly after the test begins, the CT must inform the TM.

The CT should implement appropriate controls, processes and procedures to ensure the test is carried out with sufficient assurances for all stakeholders that risks will be identified, analysed and mitigated according to industry practices in risk management. These include, but are not limited to, the inclusion of appropriate contractual safeguards in the service provision agreement with the RT provider.

The CT, in agreement with the TM, may at any time order a temporary pause if concerns are raised over damage (or potential damage). In the event of urgent issues or risks to the system, the TM will inform the TCT-SSM.

Members of the CT positioned at the higher levels of the security incident escalation chain should help to avoid miscommunication (inter alia unnecessary alerting of the relevant authorities).

5.6 Use of code names

Given the sensitive nature of the tests, and the potentially detailed findings on the weaknesses and vulnerabilities of the SI undergoing the test, all stakeholders should use code names for the test, rather than explicitly naming the SI. To the extent possible, all documentation and multilateral communication should refer to the commonly agreed code name to protect the SI's identity. This code name is to be discussed and decided in the preparation phase and defined in the initialisation documents. Code names should be chosen in such a way as to avoid revealing or disclosing any aspect of the test.

5.7 Sharing of critical issues and vulnerabilities

It is possible that, during the testing phase, a critical issue or vulnerability may be found that puts the SI in imminent danger. The CT should immediately share any such issue with the SI undergoing testing to avoid harm and allow immediate remediation. These circumstances should be discussed immediately between the CT and TM to determine the best course of action. Any information to be communicated beyond the CT should be communicated in such a way as to reveal no more than necessary about the test, while at the same time providing full transparency on the vulnerability discovered.

5.8 Joint and pooled testing

A joint test may be performed if one or more entities belong to the same group, and if certain criteria regarding, for example, ICT infrastructure, similarity, overlap and extent of CIFs, and overall feasibility are met. Any such test must (i) fulfil the requirements under DORA and the RTS on TLPT, and (ii) provide value. The ECB as TLPTA will decide whether these criteria are met either before it gives notification of the test or, in extraordinary circumstances, during the TLPT preparation phase. In

exceptional cases, the ECB may opt to perform a pooled TLPT if this is proposed by the SI, and if the ISP (and other necessary stakeholders) are willing to participate.

5.9 Supervisory cooperation

Where feasible and possible, and in order to reduce overheads for financial entities and authorities, the ECB will liaise with other relevant TLPTAs to determine whether TLPT of SIs can be carried out jointly with other financial entities and whether the authorities may have reasonable grounds for assuming the role of observer in the joint TLPT.

Annexes

A.1 Responsibility assignment matrix

Requirement	Responsible	Accountable	Consulted	Informed	Relevant documents[23]
Identification					
SI (or part thereof) is identified for TLPT	TLPTA	TLPTA	JST	n/a	n/a
Assignment of (national/SSM) TCT	TLPTA	TLPTA	n/a	TCT, SI management body	n/a
Identification letter	TLPTA	TLPTA	TLPTA	SI management body	n/a
Assignment of single point of contact (SPOC) at SI	SI management body	SI management body	n/a	TLPTA, TCT	n/a
Appointment of TM	TLPTA	TLPTA	TCT	TM, TLPTA, SPOC of SI	n/a
Preparation phase					
Notification letter	TLPTA	TLPTA	TCT	SI management body	n/a
Appointment of CTL	SI management body	SI management body	TM	n/a	TIBER-EU Control Team Guidance
Notification meeting	TM	TCT	CT	n/a	TIBER-EU Guidance for Service Provider Procurement
Initiation documents	CTL	SI management body	TM	n/a	TIBER-EU Initiation Documents Guidance
Initiation meeting	CTL	SI management body	TM	n/a	n/a
Validation of initiation documents	TM	TCT	n/a	CTL	n/a
Validation of CT composition	TM	TCT	n/a	CT	n/a

[23] Specific templates for TIBER-EU SSM tests may be used. If this is the case, the test managers will inform the control team on receiving notification that a TLPT is to be carried out.

Requirement	Responsible	Accountable	Consulted	Informed	Relevant documents[23]
Procurement process and formal contracts between the different stakeholders	CTL	SI management body	TM (non-objection)	TIP/RTT	TIBER-EU Guidance for Service Provider Procurement, contracts
Assessment of selected threat intelligence providers' and testers' compliance with DORA	TM	TM	n/a	CTL	
Launch meeting	CTL	SI management body	TM, TIP/RTT	n/a	n/a
Scope specification document	CTL	SI management body	TM	TIP/RTT, once available	TIBER-EU Scope Specification Document Guidance
Scoping meeting	CTL	SI management body	TM	TIP/RTT, once available	n/a
Approval of scope specification document	TM	TCT	JST	SI management body, CTL	n/a
Risk assessment	CTL	SI management body	TM (non-objection)	TIP/RTT	n/a
Testing phase: threat intelligence					
Scenario selection meeting	CTL, TIP	CT	TM, RTT	n/a	n/a
Scenario creation	TIP	CT	TM, RTT	n/a	n/a
Targeted threat intelligence meeting	CTL, TIP	CT	TM, RTT	n/a	n/a
Targeted Threat Intelligence Report	TIP	CT	TM, RTT	n/a	TIBER-EU Targeted Threat Intelligence Report Guidance
Approval of Targeted Threat Intelligence Report	CTL, TM	TM, CT	n/a	TIP	n/a
Testing phase: red team testing					
Red Team Test Plan	RTT	CTL	CTL, TM, TIP	n/a	TIBER-EU Red Team Test Plan Guidance
Red Team Test Plan meeting	CTL, RTT	SI management body	CTL, TM, TIP	n/a	n/a
Approval of Red Team Test Plan	TM, CT	TM, CT	n/a	RTT	n/a
Weekly test meetings or updates	RTT, CTL	CTL	TM, TIP, if requested	n/a	n/a
Leg-ups, if necessary	CT	SI management body	RTT, TM	n/a	n/a
Closure phase					
Blue team briefing	CTL	SI management body	n/a	BT	n/a
Red Team Test Report (RTTR)	RTT	CTL	n/a	BT, TM	TIBER-EU Red Team Test Report Guidance
Blue Team Test Report (BTTR)	BT	CTL	RTT	CT, RTT, TM	TIBER-EU Blue Team Test Report Guidance
Assessment of RTTR and BTTR	TM	TM	n/a	CT	n/a
Replay exercise	RTT, BT	CTL	n/a	TM	n/a
Purple-teaming exercise	RTT, BT, CTL	CTL	n/a	TM	TIBER-EU Purple Teaming Guidance
Feedback meeting	CT, RTT, BT, TIP	CTL	TM	n/a	n/a

Requirement	Responsible	Accountable	Consulted	Informed	Relevant documents[23]
Test summary report	CT	SI management body	TIP/RTT	TM	TIBER-EU Test Summary Report Guidance
Approval of test summary report	TM	TM	n/a	CT, TLPTA	n/a
Remediation plan	CT	SI management body	n/a	TM, TLPTA	n/a
Expert opinion on eligibility for attestation	TM	TM	CT, TIP, RTT	TLPTA	n/a
Attestation and test results with final submission of remediation plan	TLPTA	TLPTA	TM	JST	TIBER-EU Attestation Guidance
Integration of results into supervisory process and follow-up	JST	JST	TM	TLPTA	n/a

A.2 Abbreviations

Term	Explanation
BT	blue team
BTTR	Blue Team Test Report
CA	competent authority
CIF	critical or important function(s)
CT	control team
CTL	control team lead
DORA	Digital Operational Resilience Act
ICT	information and communication technology
JST	joint supervisory team(s)
RTS	Regulatory Technical Standards
RTT	Red Team Tester
RTTP	Red Team Test Plan
RTTR	Red Team Test Report
TIBER	threat intelligence-based ethical red teaming
TIP	threat intelligence provider
TCT	TLPT/TIBER cyber team
TCT-SSM	TCT located within the ECB tasked with TLPT tasks
TLPT	threat-led penetration testing
TLPTA	TLPT authority
TM	test manager(s)
ISP	ICT service provider
TSR	test summary report
TTIR	Targeted Threat Intelligence Report
TTP	tactics, techniques and procedures
SI	significant institution
SPOC	single point of contact

A.3 Definitions[24]

"Threat-led penetration testing (TLPT)" 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 a financial entity's critical live production systems. The TIBER-EU framework is used to implement TLPT testing requirements set out in DORA and the RTS on TLPT.

"Threat intelligence-based ethical red teaming (TIBER-EU)" is a common framework that delivers a controlled, bespoke, intelligence-led red team test of entities' critical live production systems. It enables European and national authorities to work with financial infrastructures and institutions to put in place a methodology to test and improve these entities' resilience against sophisticated cyberattacks. In particular, TIBER-EU allows for other regulatory testing requirements, such as TLPT testing under DORA, to be implemented in a standardised way that ensures a high level of quality.

"TLPT authority" means the authority in the financial sector to which the exercise of some or all of the tasks in relation to TLPT is delegated in accordance with Article 26(10) of Regulation (EU) 2022/2554, or the competent authority in accordance with Article 46 of Regulation (EU) 2022/2554.

"TLPT Cyber Team" means the staff within the TLPT authorities that is responsible for all TLPT-related matters.

"Control team" means the team that manages the test. It is composed of staff of the tested financial entity and, where relevant considering the scope of the TLPT, staff of its third-party service providers and any other party deemed relevant.

"Control team lead" means the staff member of the financial entity responsible for the conduct of all TLPT-related activities for the financial entity in the context of a given test.

"Blue team" means the staff of the financial entity and, where relevant, staff of the financial entity's third-party service providers and any other party deemed relevant in consideration of the scope of the TLPT, of the financial entity's third-party service providers, that are defending a financial entity's use of network and information systems by maintaining its security posture against simulated or real attacks and that is not aware of the TLPT.

"Test managers" means staff designated to lead the activities of the TLPT authority for a specific TLPT to monitor compliance with the requirements of DORA and the RTS on TLPT.

"Threat intelligence provider" means the experts, contracted by the financial entity for each TLPT, and external to the financial entity and to ICT intra-group service providers if any, who collect and analyse targeted threat intelligence relevant for the

[24] Definitions follow closely the ones from Article 3 of DORA and Article 1 of the RTS on TLPT.

financial entities in scope of a specific TLPT and develop matching relevant and realistic threat scenarios.

“Red Team Testers” means the testers, internal or external, contracted for, or assigned to, a TLPT.

“Purple teaming” means a collaborative testing activity that involves both the testers and the blue team.

“Leg-up” means the assistance or information provided by the control team to the testers to enable the testers to continue the execution of an attack path where they are not able to advance on their own, and where no other reasonable alternative exists, including for insufficient time or resources in a given TLPT.

“Attack path” means the route followed by testers during the active red team testing phase of the TLPT in order to reach the flags defined for that TLPT.

“Flags” are key objectives in the ICT systems supporting critical or important functions of a financial entity that the testers try to achieve through the test.

“ICT third-party service provider” means an undertaking providing ICT services.

“ICT intragroup service provider” means an undertaking that is part of a financial group and that provides predominantly ICT services to financial entities within the same group or to financial entities belonging to the same institutional protection scheme, including to their parent undertakings, subsidiaries, branches or other entities that are under common ownership or control.

“Management body” means a management body as Article 3(1), point (7), of Directive 2013/36/EU, or the equivalent persons who effectively run the entity or have key functions in accordance with relevant Union or national law.”

Postal address 60640 Frankfurt am Main, Germany
Telephone +49 69 1344 0
Website www.bankingsupervision.europa.eu

For specific terminology please refer to the SSM glossary (available in English only).

PDF ISBN 978-92-899-7456-1, doi:10.2866/2818545 QB-01-25-228-EN-N