EUROPEAN CENTRAL BANK

TIBER-EU FRAMEWORK

How to implement the European framework for Threat Intelligence-Based Ethical Red teaming

January 2025

Contents

1 Executive summary

1.1 What is TIBER-EU?

The Framework for Threat Intelligence-based Ethical red teaming (TIBER-EU) provides a uniform and high-quality standard for implementing realistic intelligence-led red team tests on live production systems throughout (and beyond) the European Union. It delivers a controlled, bespoke, intelligence-led red team test of entities' critical or important functions (CIFs), and the underlying systems supporting these CIFs, i.e. people, processes and technologies, and mimics the tactics, techniques and procedures (TTPs) of real-life threat actors. TIBER-EU enables European and national authorities to work with financial and other entities (hereafter referred to collectively as "entities") to put in place a programme to test and improve their resilience against sophisticated cyber-attacks. It can help entities to assess their protection, detection, and response capabilities.

1.2 What are the core objectives of TIBER-EU?

As the appetite grows for authorities in different jurisdictions to develop national intelligence-led red teaming frameworks, and with the inclusion of such type of tests in regulation, there is a risk that incompatible frameworks emerge which could lead to fragmentation and duplication of effort. Multiple frameworks potentially represent a substantial burden for the respective entities and may lead to inconsistent results. TIBER-EU therefore has the following core objectives:

- enhance the cyber resilience of entities and of the financial sector;
- standardise and harmonise how intelligence-led red team tests are performed in the EU, while also allowing each jurisdiction a degree of flexibility in the implementation of the framework by adding its national specificities;
- provide guidance to authorities on how they might implement and manage this form of testing at a national or European level;
- help entities and authorities to fulfil the requirements to perform Threat-Led Penetration Tests (TLPT) as per established regulation(s) in a safe manner, through the use of TIBER-EU. For example, Regulation (EU) 2022/2554, referred to as the Digital Operational Resilience Act (DORA). The TLPT-related requirements under DORA are included in the detailed TIBER-EU testing process, so that financial entities completing a test under a national or European-level implementation of the TIBER-EU framework will be DORA TLPT-compliant, assuming they fulfil the formal TLPT-related requirements set by the competent authorities. The TIBER-EU framework may be used as a handbook or set of detailed guidelines on how to complete DORA TLPT in a qualitative, controlled and safe manner – one which is consistent and uniform throughout the EU[1];

[1] See for further information: 'Adopting TIBER-EU will help fulfil DORA requirements', September 2024, available at: https://www.ecb.europa.eu/press/intro/publications/pdf/ecb.miptopical240926.en.pdf

- support cross-border, cross-framework intelligence-led red team testing for multi-jurisdictional entities;
- foster mutual recognition of tests across the EU jurisdictions, by relying on test results and collaborating on joint tests, thereby reducing the regulatory burden on entities and authorities;
- catalyse information sharing and the joint analysis of test results.

1.3 Who is the framework for?

This framework document provides an overview of TIBER-EU and how it can be implemented across the EU, with details of the key phases, activities, deliverables and interactions involved in a TIBER-EU test. The document is aimed at:

- authorities responsible for the adoption, implementation and management of the TIBER-EU framework at national and European levels;
- entities looking to undertake voluntary TIBER-EU tests;
- entities using this framework as operational guidance for performing TLPT as required by the Regulation (EU) 2022/2554, referred to as the Digital Operational Resilience Act (DORA);
- supervisors and overseers of above-mentioned entities;
- providers interested in providing cyber threat intelligence services and red team testing services under TIBER-EU.Red Team Testers (RTT) interested in providing red team testing services under TIBER-EU.

The TIBER-EU framework is designed to be used for entities that carry a certain degree of systemic importance at national or at European level, and are sufficiently mature from an ICT perspective. However, the framework itself can be used by any type or size of entity across the financial and other sectors.

1.4 Who are the key stakeholders involved in the adoption and implementation of TIBER-EU tests?

The TIBER-EU framework is designed to be adopted and implemented by relevant national authorities in any jurisdiction, as well as at European level, from a variety of perspectives. For instance, the framework may be implemented from a catalyst perspective to promote resilience across the financial sector, for financial stability purposes, or as a supervisory/oversight tool. The respective TIBER authorities[2] and

[2] A TIBER authority is any authority under the TIBER framework and/or its national or European implementations, conducting (regulatory) tasks within a TIBER test. When using the TIBER-EU framework for TLPT obligations under DORA, the respective “TLPT authorities” are considered as TIBER authorities for that test.

TIBER Cyber Teams (TCTs)[3] will then consider which entities could be invited to undergo a TIBER-EU test, also taking into account the voluntary interest expressed by the entities themselves.

TIBER-EU engages the following key stakeholders:

- the entity[4], which is responsible for managing the end-to-end test and ensuring that all risk management controls are in place to facilitate a controlled test;
- the TIBER authority(ies)[5], which is responsible for adopting and implementing TIBER-EU, closely monitoring and guiding the test and ensuring it is conducted in the right spirit and in accordance with the requirements of the TIBER-EU framework;
- the Threat Intelligence Provider (TIP) who provides threat as well as target intelligence; and
- the Red Team Testers (RTT), who execute the attack scenarios.

For the TIBER-EU test to provide meaningful results, it is important that all stakeholders work closely together, in a spirit of trust and cooperation. The test will not result in a 'pass or fail'; rather, it will provide all parties with an insight into strengths and weaknesses, and enable the entity to learn and evolve to a higher level of cyber maturity.

1.5 What are the risks of a TIBER-EU test?

There are inherent elements of risk associated with a TIBER-EU test due to the criticality and importance of the live production systems, people and processes involved in the tests. 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. Accordingly, the TIBER-EU framework places high priority on establishing robust risk management whereby risks are identified, assessed and managed at all times to ensure the test is conducted in a controlled and safe manner, adhering to the highest standards. In addition, the tester and provider requirements under the TIBER-EU framework have been made deliberately stringent to ensure that only the most competent, qualified and skilled personnel with the required experience conduct such sensitive tests on CIFs.

1.6 How to implement TIBER-EU?

The authorities of jurisdictions considering to adopt TIBER-EU may liaise with each other as well as with their respective entities to determine how best to adopt and implement the framework. A jurisdiction formally adopts TIBER-EU by

[3] A TIBER Cyber Team (TCT) comprises staff within the TIBER authority that is responsible for coordinating and managing TIBER-related activities – most importantly the testing of entities.

[4] A TIBER test may involve more than one entity, see also section 3.7 on multi-party testing.

[5] A TIBER test may involve more than one TIBER authority, see also section 3.7 on multi-party testing.

communicating to the industry the implementation of the national TIBER-XX[6], and by publishing an implementation document that includes national specificities, if any.

The TIBER-EU framework envisages a collaborative approach, with all stakeholders working closely together and learning from each other. The implementation of the TIBER-EU framework by national or European jurisdictions is monitored by the secretariat of the TIBER-EU Knowledge Centre[7] (TKC). In addition, the TKC reflects and integrates learnings from all jurisdictions to evolve and improve the framework.

Any further enquiries about the TIBER-EU framework should be directed to TIBER-EU@ecb.europa.eu. Questions regarding local TIBER implementations may be referred to the TIBER-XX contact points of the national or European TIBER authorities. Additional documents, which provide more specific guidance and templates during the testing process, can be found at the TIBER-EU webpage.

[6] Where XX stands for the respective country code (e.g. DE, FR, NL, etc.), see paragraph 2.2.1.

[7] More information on the TKC can be found in paragraph 2.2.2.

2 Adoption and implementation of TIBER-EU

2.1 Background and purpose

The financial system is a complex network of participants from different environments and shared technologies, with a large volume of information flowing through the network. It includes all types of entities, information, technologies, rules and standards that enable financial intermediation. Efficient, safe and reliable infrastructure enables entities and others to expand their offering of financial services to the broader economy. Within this context, there are highly sophisticated cyber threat actors who target the most vulnerable links in this network. Hence, it is critical that entities reduce their vulnerabilities at every point and strengthen their overall resilience. This requires diverse, layered approaches, solutions and tools. Intelligence-led red team testing is one such tool to help entities test and enhance their protection, detection and response capabilities.

TIBER-EU enables authorities to work with entities under their responsibility to put in place a programme for testing and improving their resilience against sophisticated cyber-attacks. TIBER-EU can also be used as additional operational guidance for complying with supervisory testing obligations[8].

For the purposes of the TIBER-EU framework, “entities” include (but not limited to):

credit institutions, payment institutions, electronic money institutions, payment systems, central securities depositories, central counterparties, trading venues, insurance and reinsurance undertakings, settlement platforms, and any other service providers and financial entities identified based on their systemic importance and ICT risk profile.

This framework document provides an overview of how TIBER-EU is to be implemented. It explains the key phases, activities, deliverables and interactions involved in a TIBER-EU test. This overarching framework document should be complemented with the other available TIBER-EU documentation.

2.1.1 Why intelligence-led red team testing?

Penetration tests provide a detailed and useful assessment of technical and configuration vulnerabilities, often within isolation of a single system or environment. However, they do not assess the full scenario of a targeted attack against an entire entity (including the complete scope of its people, processes and technologies).

To provide an appropriate level of assurance that the CIF’s and their underlying systems are protected against technically competent, resourced and persistent adversary attacks, the level and sophistication of testing must be increased, and the testers must be armed with up-to-date and specific threat intelligence.

[8] Such as TLPT under DORA.

An intelligence-led red team test mimics the TTPs of real attackers on the basis of bespoke threat intelligence. In doing so, it looks to target the people, processes and technologies underpinning the CIFs of an entity in order to test its protection, detection and response capabilities. Such a test allows the entity to understand its real-world resilience by stressing all elements of its business against the TTPs of threat actors that may be targeting its organisation.

The intelligence-led red team test provides a comprehensive end-to-end understanding of weaknesses present in people, processes, technology, and their associated intersection points, and provides a detailed threat assessment which can be used to further enhance the entity's situational awareness.

The idea of TIBER-EU is to:

- bring together the best available threat intelligence, tailored to the business model and operations of a particular entity, to set up credible scenarios mimicking the key potential attackers and the attack types they would deploy;
- use this intelligence to enable ethical RTT to mimic more accurately real-life attacks from competent adversaries on the live production systems of the entity.

TIBER-EU tests are to be performed without the prior knowledge of the target entity's security or response capability, i.e. Blue Team (BT). Only a small group of representatives from the entity, referred to as the Control Team (CT), know about the test. This is to ensure that the test can assess how effectively the target entity is able to protect its CIFs and underlying systems, and how effectively it can detect and respond to attacks.

Given the nature of a TIBER-EU test and the critical nature of the live production systems and other connected environments being tested, the framework sets out a number of risk management activities to ensure a controlled test. More information on risk management can be found in chapter 4 of this framework.

Because of the resources required and costs incurred, entities are not expected to conduct a TIBER-EU test too frequently – with 3 years intervals being the norm.

2.2 Implementation of the TIBER-EU framework

The adoption of the TIBER-EU framework by authorities and jurisdictions is voluntary, although the framework may be used to provide additional operational guidance on how to comply with legal obligations stemming from applicable legislation. At the inception, authorities wishing to implement a TIBER-EU framework in their jurisdictions are encouraged to liaise with all relevant authorities in the financial sector. These may include:

- central banks;
- competent authorities (e.g. supervisors or overseers);
- intelligence agencies;
- relevant ministries.

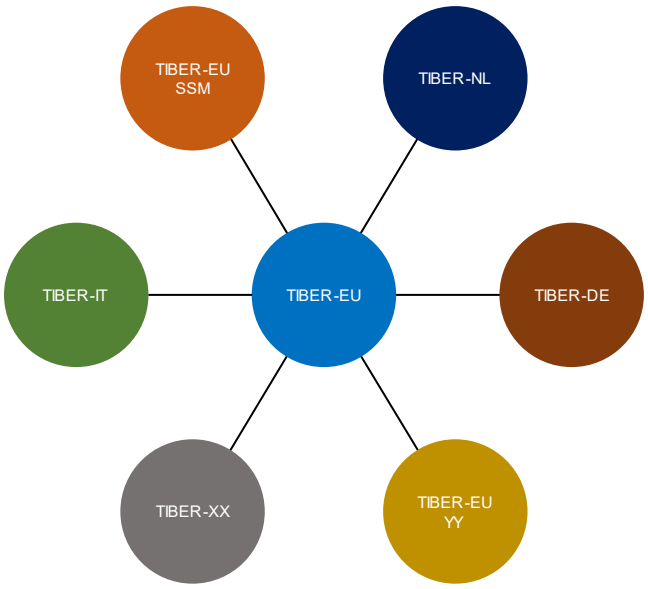
The TIBER-EU framework may be adopted at a national level, or by EU institutions and authorities. However, a national or European implementation of TIBER-EU does not need to be limited to the financial sector alone. Should a jurisdiction wish to involve other sectors (such as telecommunications, utility companies), the TIBER-EU framework does not prevent it from doing so. As such, the framework is entity-agnostic and sector-agnostic.

The various authorities should discuss the potential adoption of the framework, how it should be set up, the entities that it will apply to, the timelines, and the general organisation and resources required to implement the framework.

2.2.1 National or European implementation

The TIBER-EU framework constitutes a common foundation. Each jurisdiction that adopts the framework can apply it in a manner which suits its specificities, whilst adhering to the mandatory requirements of TIBER-EU. If the framework is adopted at a national or European level, there should be an accompanying national (TIBER-XX) or European (TIBER-EU YY) implementation document, with XX representing the two-letter ISO 3166-1 country code and YY the European authority. This abstraction is illustrated in figure 1 below. Note that all current implementations of TIBER-EU can be found on the TIBER-EU webpage.

Figure 1
TIBER-EU framework and national/European implementation documents



The implementations displayed in figure 1 are examples and do not exhaustively represent all implementations of TIBER-EU.

If a jurisdiction decides to adopt the TIBER-EU framework, the TKC must be officially informed that a national or European implementation of TIBER-EU has been launched.

On adoption, the TIBER authority (or authorities) that takes ownership of the TIBER-XX or TIBER-EU YY implementation document within the jurisdiction, must publish it

on its website(s), and take measures to explain the adoption of the framework to the relevant market participants. The national implementation must be formally adopted by the Board of the authority.

The implementation document should include, at a minimum:

- a statement that TIBER-EU has been implemented by the respective jurisdiction (or in the respective European context);
- the target sectors in scope of testing;
- information on the respective TIBER authorities and TCTs, including the relevant contact details;
- information on national or European implementation specificities;
- reference to TIBER-EU documentation.

Each implementation of TIBER-EU must ensure that all the core foundational concepts and approaches are adopted and implemented. The framework offers a level of flexibility which allows for national implementations to accommodate a wide range of institutional set-ups, legal mandates, and market structures. Therefore, jurisdictions may provide further advice on implementation as well as operational aspects of testing in national guidelines, always in line with the intent and spirit of the framework. Alternatively, jurisdictions may just refer to the TIBER-EU documentation as their own implementation when publishing the national implementation document, which shall include the minimum content specified above.

The TKC ensures that all implementation documents are in accordance with the TIBER-EU framework and are compatible among themselves. In any case, the implementation of the TIBER-EU framework must be in accordance with the mandatory requirements, as set out in annex 10.2.

For each national and European implementation of the TIBER-EU framework, the TIBER authorities should establish the appropriate governance structures and allocate resources to:

- ensure that the implementation document is formally owned by senior management;
- manage, operationalise and monitor its implementation by staff with the requisite skills;
- continuously update the implementation document in the light of lessons learned from its implementation, and in collaboration with other TIBER authorities via the TIBER-EU Knowledge Centre.

2.2.2 TIBER-EU Knowledge Centre

A centralised TIBER-EU Knowledge Centre (TKC), hosted by the ECB[9], enhances further collaboration among authorities and TCTs, so that they can benefit from the

[9] In close cooperation with the European System of Central Banks (ESCB).

various implementations of the TIBER-EU framework. The core objectives of the TKC are to:

- facilitate knowledge exchange and foster collaboration among national and European TCTs and other stakeholders;
- support national and European implementations, and provide a central depository of materials for jurisdictions;
- provide authorities with training on the development, implementation and management of the TIBER-EU framework;
- monitor the national and European implementations (thereby ensuring legitimacy of mutual recognition), collect feedback, reflect on lessons learned, disseminate information to national jurisdictions as appropriate, and maintain and continually develop the TIBER-EU framework;
- promote information sharing, mutual collaboration and other actions to enhance overall cyber resilience within the EU;
- liaise with other authorities using intelligence-led red team testing in order to promote international uniformity and quality;
- provide feedback to the sector within the relevant fora (e.g. Euro Cyber Resilience Board for pan-European Financial Infrastructures), where necessary and appropriate;
- act as a hub, where TCTs can liaise and coordinate in advance when initiating multi-jurisdictional tests.

2.2.3 Identification of entities and relevant authorities

As a general rule, the TIBER authority that wants to adopt the TIBER-EU framework and drafts the national or European implementation document should initiate and oversee the conduct of TIBER-EU tests on entities under its responsibility.

Following the adoption of the TIBER-EU framework at a national or European level, the TIBER authority, or authorities where applicable, should decide which entities should be invited to undertake, or must undertake, a TIBER-EU test, and by when. Entities differ in size, complexity and reach. Therefore, TIBER authorities should look to include entities which are important to the financial stability of the jurisdiction based on the CIFs they perform. Where more than one entity (e.g. belonging to the same group) are sharing the same significant ICT infrastructure, TIBER authorities may allow the conduct of a joint test.

2.2.4 Legal and compliance

During the process of establishing the implementation of TIBER-EU, authorities should conduct a review of existing laws and regulations at a national and European level to ensure that the framework, methodologies and processes do not contravene any law – and the implementation of the framework remains legally compliant.

During the TIBER-EU process, there are several activities that may be performed to mimic a real-life attack. Such activities require due consideration and evaluation in the context of existing laws and regulations. These activities may include the following:

- gathering open-source intelligence (OSINT) data on the target entity, its suppliers, its employees and/or its customers (publicly available information);
- gathering data from other intelligence sources (e.g. government sharing platforms, etc.) and the dark web relating to the target entity, its suppliers, its employees and/or its customers;
- gathering account and password data from employees and service providers of the target entity.
- deployment of people into the entity under various guises to gather intelligence;
- using targeting data gathered in the threat intelligence phase to create email, telephone and in-person ruses as part of a scenario;

The above list is not exhaustive. Entities should ensure that a thorough legal analysis is carried out, using appropriate legal expertise, to determine the legal constraints when performing the test. Naturally, the above activities will be performed under contractual agreement with the full consent of the respective entity. This will mitigate many of the legal concerns which may arise.

Simultaneously, all participating parties should consider and act in accordance with the legal constraints of each jurisdiction and are prohibited to perform illegal and unethical actions, not limited to the listed actions under paragraph 4.1.4.

3 Stakeholders and cooperation

3.1 Stakeholders in a TIBER-EU test

A TIBER-EU test requires the involvement of a number of different stakeholders, with clearly defined roles and responsibilities. These are:

- TIBER Cyber Team(s) (TCT) and Test Manager(s) (TM);
- Control Team (CT) and Control Team Lead (CTL);
- Blue Team (BT);
- Threat Intelligence Provider (TIP);
- Red Team Testers (RTT);

All stakeholders involved in a TIBER-EU test should be well-informed about their respective roles and responsibilities, to ensure that:

- the test is conducted in a safe and controlled manner;
- the information flow protocol is clear on how information will be stored and shared between stakeholders.

The end-to-end conduct of a TIBER-EU test is the responsibility of the tested entity. The two stakeholders involved in project management are the TM and the CTL. Both the TM and CT should have extensive knowledge of the entity's business model, functions and services.

All parties involved in a TIBER-EU test should take a collaborative, transparent and flexible approach. It is critical that all relevant stakeholders keep each other informed at all stages to ensure that the test runs smoothly – and that any issues, resourcing constraints, etc. can be addressed in a timely fashion.

For a structured view on the roles and responsibilities of the different stakeholders involved in the overall process of a TIBER-EU test, please refer to the RACI Matrix included in annex 10.1.

3.2 The TIBER Cyber Team

The TIBER authorities implementing the TIBER-EU framework should set up a TCT that brings together their TIBER knowledge and capabilities at national or European level. A TCT is composed of staff involved with TIBER-EU related matters, including TMs. Apart from TMs, the TCT may include subject matter experts, thus providing additional knowledge and best practices for the conduct of the tests.

There are various ways in which the TCT could be set up, ranging from one TIBER authority alone to a transversal team consisting of experts from different TIBER authorities within a given member state. Most importantly, the TCT is one of the crucial operational controls in performing a test on critical and important live

production systems, and helps ensure a uniform, high-quality test containing all the mandatory elements. The TCT should be in a position to fulfil the following tasks:

- maintain the national/European TIBER implementation document and develop it further according to national or European needs;
- facilitate TIBER tests;
- act as the contact point for all external enquiries regarding the national TIBER implementation;
- where applicable, support the overseers and supervisors during and/or after the tests (if the overseers and supervisors are not included in the TCT);
- achieve pan-European convergence by liaising with other TCTs and participating in TKC activities for TM training, best practices sharing, presentations and trainings for authorities, providers and tested entities.

When setting up the TCT, each jurisdiction should carefully consider the resources required, based on the number of entities that will be subject to testing. To safeguard the effectiveness and learning effect of the test, it is strongly encouraged that the members comprising the TCT are not involved in a test in their supervision or oversight capacity.

3.3 The Test Manager

For each TIBER-EU test, there should be a dedicated TM, and at least one alternate from the TCT, who has experience in the relevant sector, as well as cyber expertise and project management experience. The role of the TM is to make sure that the entity undertakes the test in a uniform and controlled manner, and in accordance with the TIBER-EU framework and applicable requirements[10]. For the conduct of the test, the TM may be supported by other members/experts of the TCT for specific process steps.

Although the CTL is the primary contact for the TIP and RTT, the TM should also have direct access to them when required. If there are significant deviations in the original planning of the test, this should be discussed with the TM. Where there are crucial decisions to be made (e.g. deviations during the test from the agreed scope) and no consensus is reached between the stakeholders, both the CTL and TM should have a formal escalation line to their respective superiors. These formal lines may consist of:

- the entity's chief information security officer, chief operating officer, chief risk officer or any other appropriate senior personnel with sufficient decision-making authority;
- the head of the TCT, or any other appropriate senior personnel with sufficient decision-making authority.

[10] For operational decisions during tests, such as the approval of deliverables, the TM is equated with the TIBER authority – as the TM is the actor involved in day-to-day operational tasks during tests.

The TM is independent from the CT and is not accountable for the CT's actions, the running of the test, and the outcomes or the remediation planning. During a TIBER-EU test, the TM holds the right to invalidate a test for TIBER recognition if the entity is not conducting the test in the right spirit or in accordance with the mandatory requirements of the TIBER-EU framework. In such a case, no attestation will be provided, and the test will thus not be recognized in other TIBER jurisdictions.

The TM will inform the CTL as soon as possible if a risk of non-attestation emerges, to provide potential recourse, if possible. Should a test be invalidated, the entity can choose to continue the test to gain insight and enhance their learning experience, without it being recognized as a TIBER-EU test. Indicative situations in which the TM may invalidate the test are when:

- either the TIP or the RTT has (repeatedly) shown it does not fulfil its role as required per the TIBER-EU framework and/or the TIBER-EU Guidance for Service Provider Procurement (GSPP) and applicable requirements for testers;
- a test has been compromised by the RTT and/or TIP and/or the entity, either intentionally or as a result of (gross) negligence;
- there is (a strong indication of) foul play by any of the involved parties;
- the quality, safety or the secrecy of the test is compromised.

3.4 The Control Team and Control Team Lead

For each TIBER-EU test, there should be a CT, with a dedicated CTL from the entity. The CT (or a member of the CT) should be positioned in such a manner that they can ascertain any information regarding detections by the BT and/or by ICT third party service providers in use.

Responsibility for the overall planning and management of the test lies with the entity. The CTL is responsible for determining and finalising the scope and its board approval, the scenarios and risk management controls for the test, ensuring that they have been validated by the TM. In addition, the CTL should coordinate all test activity including engagement with the TIP/RTT and authorities. The CTL should ensure that the TIP/RTT's project plans are factored into the entity's overall project planning for the TIBER-EU test. Given the importance of the CTL's role, a backup CTL is strongly advised. More details on the roles, responsibilities and ideal composition of the CT can be found in the TIBER-EU Control Team Guidance (CTG).

Close cooperation between the CTL and TM is required during all phases of the test. The CT shall provide any information regarding the test to the TM upon request.

3.5 The Blue Team

For each TIBER-EU test, the BT comprises all staff at the entity, the entity's third-party service providers and any other party deemed relevant in consideration of the scope of the test, who are not part of the CT and are not aware of the test. More

specifically, the BT is defending a financial entity's use of network and information systems by maintaining its security posture against simulated or real attacks. It is critical that the BT be completely excluded from the preparation and conduct of the TIBER-EU test. During the closure phase, when the BT is informed about the conduct of the test, the relevant and appropriate members of the BT should participate in the replay, Purple Teaming (PT) and remediation exercise, including the respective follow-up.

3.6 The TIBER-EU Service Providers

In TIBER-EU, it is mandatory to use an external TIP and strongly encouraged to use external RTT, as there are clear advantages to procuring an external party to conduct the test. Notably, external RTT provide a fresh and independent perspective, which may not always be feasible with internal teams that have grown accustomed to the internal systems, people and processes. Furthermore, external RTT may have more resources and up-to-date skills to deploy, which would add value to the test.

In exceptional circumstances, and only after the prior approval by the TM, internal RTT may be used for a TIBER-EU test[11]. In such cases, internal testers need to adhere to the same standards and requirements as external RTT. Testers employed by an ICT intra-group service provider are considered as internal testers.

At all times, the TIP and the RTT must work closely with each other during the TIBER-EU test. This includes providing and transforming targeted threat intelligence (TTI) information into end-to-end attack scenarios for the Red Team testing, as well as liaising on new and updated intelligence as the Red Team test progresses and updating the threat intelligence assessment and attack scenarios if needed. The RTT must demonstrate a willingness to work closely with the TIP, which includes reviewing and commenting on the intelligence deliverables (once approved by the entity) as well as transforming threat scenarios into a cohesive and tractable Red Team Test Plan (RTTP). The RTT should indicate various creative options in each of the attack phases based on the various TTPs used by advanced attackers. This anticipates for changing circumstances or in case other attack methods do not succeed during the test. The RTT are expected to liaise and work with the TIP throughout the testing in order to update the threat intelligence assessment and attack scenarios with relevant and up-to-date intelligence. The scenario development is a creative process, and TTPs should not simply mimic scenarios seen in the past but should look to combine the TTPs of various relevant threat actors.

3.6.1 The Threat Intelligence Provider

The TIP should provide threat intelligence to the entity in the form of a Targeted Threat Intelligence Report (TTIR), which can be further enriched by the RTT. The TIP should use multiple sources of intelligence to provide an assessment that is as accurate and up to date as possible. The TTIR sets out the threat scenarios that, together with the RTT, are developed into attack scenarios. The TIP is also expected to provide input into the final Red Team Test Report (RTTR) issued to the entity.

[11] Significant credit institutions as identified under DORA cannot use internal testers.

The TIP must cooperate with the RTT during the remainder of the TIBER-EU test. This includes helping to develop the attack scenarios for the Red Team test, as well as any new intelligence requirements that occur as the Red Team test progresses. The TIP is expected to provide input into the final report issued to the entity.

3.6.2 The Red Team Testers

The RTT should aim to assess the cyber resilience posture of the entity in the light of the threats it faces. The RTT plan and execute attacks on the target systems and services, which are agreed in the scope. The RTT should indicate various creative options in each of the attack phases based on the various TTPs used by advanced attackers. This anticipates for changing circumstances or in case other attack methods do not succeed during the test. The RTT drafts a RTTR including identified issues during the test.

The RTT should follow a rigorous and ethical Red Team testing methodology, and meet the minimum requirements defined under the TIBER-EU framework. The rules of engagement and specific testing requirements should be established by the RTT and the entity.

3.6.3 Working with internal Red Team Testers

The exceptional use of internal testers needs to be approved by the TM. Before approving the use of internal testers, the TM should:

- assess that internal testers have sufficient resources and capabilities available to perform a TIBER test;
- assess that the entity has shown that conflicts of interest are avoided throughout the design and execution phases of the test;
- consider the requirements for the external testers as laid down in the GSPP, in particular chapter 2;
- ensure that the entity did not conduct two consecutive TIBER tests using internal testers, prior to this engagement.

For the approval by the TM, the entity must attest that:

- the use of internal testers will not negatively impact the entity's general defensive or resilience capabilities regarding ICT-related incidents, or significantly impact the availability of resources devoted to ICT-related tasks during the test;
- the members of the internal testing team are not part of an incident team or in other ways would work with BT related activities in case of an incident;
- the entity has capable back-up resources or a contract with an external party to provide extra resources if a member of the internal testing team for any reason won't be able to work as much as planned with the test;

- the use of internal testers does not add any significant risk of the test being discovered;
- the entity has an active and capable CT and should not move CT tasks to the RTT;
- the use of internal testers does not negatively impact the flow of information during the testing phase, e.g. during the status meetings.

When using internal testers in the context of TIBER, it is complicated to handle their internal knowledge. Internal testers will, for example, have an advantage in knowing the detection capabilities of the entity, thus changing the black-box/grey-box approach of the test. There may also be a higher risk for lack of transparency when using internal testers, since the testers know the internal environment / processes. Instead of using only internal testers, the recommendation is to have at least an experienced external RT test manager join the internal testers. This brings a fresh and independent perspective to the test, facilitates further development of the internal RTT, and provides additional experience with testing the entity's production system. The entity should have a policy in place for the management of internal testers. Such policy shall:

- include criteria to assess the suitability, competence, and potential conflicts of interest of the testers. The policy defines management responsibilities in the testing process, and the policy shall be documented and periodically reviewed;
- provide that the internal testing team includes a test lead, and at least two additional members. The policy shall require that all members of the test team have been employed by the entity or by an ICT intra-group service provider for the preceding 12 months;
- include provisions for the internal testers on regular training on how to perform penetration testing and red team testing.

3.7 Multi-party testing

While there is typically only one TIP and one team of RTT during a TIBER test, the extent of the test may not be limited to a single party[12]. On the contrary, the underlying ICT infrastructure of a tested entity is often complex and distributed in nature, requiring the inclusion of subsidiaries, critical service providers (CSPs) or even additional entities. The inclusion of such additional parties leads to a significantly increased need of coordination to keep the test manageable and efficient. Additionally, the test might require the inclusion of several TMs belonging to different TCTs.

In this section, principle-based advice is provided for tests including multiple parties. This advice should be further adapted and tailored on a test-by-test basis.

When conducting multi-party testing, the following general principles should be considered:

[12] A "party" is considered to be any legal entity being involved in the scope of a TIBER test, irrespectively of whether it's an financial entity (e.g. FMI, credit institution, insurance institution) or any other legal entity (e.g. service provider, non-financial sector entity).

- For a multi-party test to generate value and learning, the involved entities must all rely on common ICT systems in substance, in particular those underpinning CIFs.

- The organisation and execution of a test might become very complex with an increased number of involved parties. It is therefore recommended to limit the number of parties involved in a test. There should be a designated CT forming the lead of the involved parties.

- Proper scope definition is key for multi-party testing, conducting a comprehensive analysis on which entities – as well as authorities – are to be included in a test. Moreover, which CIFs and systems of the scope are implemented by which party, and how many scenarios are to be tested for each entity (including entity-overarching scenarios). The number of scenarios, the duration of the active testing and the allocated resources for the TIP/RTT should be proportionate to the number of entities involved in the test.

- Communication and documentation need to be set up in a way to adequately include all necessary parties. For example, establishing clear and comprehensive communication and document distribution, as well as decision-making and escalation procedures. It should be decided if documents are submitted separately for each tested entity, or in a combined form. Agreements and decision-making on different levels might be structured more efficiently. Namely, by CTs aligning amongst themselves during pre-discussion meetings, before getting together with the TCT and service providers.

3.7.1 Multi-jurisdictional tests

TIBER tests might require the collaboration of more than one TCT. This typically occurs when entities operate their business across borders, with a presence in multiple jurisdictions. Under such circumstances it needs to be considered if the TCTs of the respective authorities would like to assign TMs to the test. The TIBER-EU framework permits for the involvement of members of multiple TCTs into a TIBER test.

When conducting a multi-jurisdictional test, the following general principles should be considered:

- All relevant TCTs to be involved should be considered adequately. TCTs might be identified via the tested entity, providing a list of countries it has relevant business in, by inquiries into the focus lists of other TCTs, or through information on the entity's business footprint from respective competent authority.

- If a jurisdiction within the scope of a TIBER test has not yet implemented TIBER, the relevant competent authority might be inquired to check if there are other legislative testing obligations[13]. If there are no other testing obligations or TIBER implementations, the entity's critical infrastructure of

[13] E.g., they might still be obliged to undergo testing under regulatory obligations, in that case a TIBER & regulatory framework-coordinated test is advised when feasible.

that jurisdiction may be included in the TIBER test regardless of the missing implementation.

- The relevant TCTs are encouraged to liaise with each other in order to determine the lead TCT for the test, taking into account factors such as the home member state of the entity, the CIFs to be tested and the order of test initiation. TCTs should align upfront regarding national testing particularities and agree on the formal test requirements, e.g. meetings conducted in addition to the ones mandated by the TIBER-EU framework, formal requirements, etc.

- Similar to multi-party testing, an efficient test organisation and execution requires the limitation of additional TCTs involved in the multi-jurisdictional test. This can be achieved by applying tiered participation, assigning roles to each involved TM of the respective additional TCTs, using the following exemplary roles:

    - Lead: The TM of the lead TCT is the principal facilitator of an expedient and efficient decision-making process, and involves other TMs according to their respective role.

    - Participant: The TM of the additional TCT participates in meetings and receives relevant documents, as well as participates in the decision-making processes.

    - Observer: The TM of the additional observing TCT, at minimum, will receive the scope specification document, the test summary report, the remediation plan and the attestation. Additional involvement can be agreed upon.

    - No involvement: The additional TCT is not involved in the testing meetings and the decision-making process[14].

3.7.2 Mutual recognition

In the highly interconnected European financial system, it is likely that numerous authorities will require assurance on the cyber resilience of a single entity. TIBER-EU provides an efficient solution to this problem by ensuring mutual recognition of TIBER tests, provided that these comply with all mandatory requirements of the TIBER-EU framework.

At the end of each test, the TM leading the test will sign an attestation confirming that the test was conducted in accordance with the mandatory requirements and the spirit of the TIBER-EU framework, in addition to the national or European implementation document. This attestation provides the grounds for mutual recognition.

[14] If the TIBER-EU framework is used for a test based on a mandated regulatory exercise, there might be additional reporting obligations the entities' competent authorities will have to receive from the entity: the test summary, the remediation plan as well as the attestation.

4 Risk management for TIBER-EU tests

4.1 Risk management

The TIBER-EU test harbours elements of risk for all parties, owing to the criticality of the target systems, the people and the processes involved in the tests. The possibility of causing a denial-of-service incident, an unexpected system crash, damage to critical or important live production systems, or the loss, modification or disclosure of data highlights the need for active and robust risk management.

Throughout the conduct of the TIBER-EU test, the entity should ensure that it gives due consideration to the risks associated with the testing of live production systems of CIFs, including potential impacts on the financial sector, as well as on financial stability at European and national level.

Entities should conduct thorough due diligence of in-scope systems prior to any testing, to ensure that backup and restoration capabilities are in place.

4.1.2 Risk assessment

Ultimately, the entity is responsible for the red team test and the risks that stem from it. The CT should therefore remain in control of the testing process, as well as continuously manage the relevant risks in an effective manner.

The CT should conduct a risk assessment before and during the test. The risk assessment should be well documented, reviewed and updated when needed, such as when the attack scenarios have been developed. Before the testing phase commences, the CT should consult the TM on the risk assessment. Risks to be considered – among others – relate to:

- the procurement of providers;
- the level of confidential data to which these providers gain access;
- crisis and incident escalation;
- the interruption of critical activities and/or impact of provider activities on the entity and its third parties;
- the incomplete restoration of systems affected by the test.

When several entities are involved in a multi-party test, the CT of each entity shall conduct its own risk assessment, also taking into consideration the services offered by ICT third party service providers. The CT of the entity assigned to direct the test shall also conduct the risk assessment for the aspects of the test specific to the involvement of several entities. Moreover, the CT of the involved entities should work together to identify potential joint risks, including those related to the use of a common ICT third party service provider and the offered services (e.g. regarding a single point of failure).

4.1.3 Minimum requirements for providers

A key means of managing the risks associated with the TIBER-EU test is to use the most competent, qualified and skilled TIP and RTT with the required experience to conduct such tests. Consequently, prior to the engagement, the entity must ensure that the TIP and RTT are free from conflict of interest and meet the minimum requirements evidenced by the relevant documentation and certifications. The minimum requirements are set out in the GSPP. Where feasible, entities should ensure that the providers are accredited and certified by a recognised body as being able to conduct a TIBER-EU test.

4.1.4 Contracts

The contracts[15] with the TIP and RTT should include:

- a requirement for the providers to meet security and confidentiality standards at least as stringent as those followed by the underlying entity;
- the protection of parties involved (e.g. indemnifications);
- a clause related to data destruction requirements and breach notification provisions;
- activities that are not allowed during the test, such as: unauthorised destruction of equipment, uncontrolled modification of information and ICT assets, intentional compromise of the continuity of CIFs of the tested entity, unauthorised inclusion of out-of-scope systems, unauthorised disclosure of test results, blackmail; threatening or bribing employees.

In case of a multi-party test, the same external RTT and TIP shall be used for the purpose of conducting the test. The testing entity and the other participating entities should have a mutual agreement on the aspects above with the selected TIP and RTT. The GSPP set out in greater detail agreement checklists for the entity and TIP/RTT to consider when formalising their contractual agreements.

4.1.5 Confidentiality and escalation procedures

Protecting the confidentiality of the test is crucial to its effectiveness. To that end, the entity should limit awareness of the test to a small, trusted group on a need-to-know basis, whose members have the appropriate levels of seniority to make risk-based decisions regarding the test.

The entity should clearly define which measures are to be taken to ensure that only the CT is informed about the test (e.g. CT members may sign a non-disclosure agreement (NDA) to ensure their confidentiality throughout the test).

The CT should define escalation procedures to avoid the triggering of actions that would be mandatory in the case of a real event, and contain such actions when

[15] These requirements also apply when working with internal RTT and should therefore be documented accordingly.

needed. Such actions include communicating with an external party, e.g. a computer security incident response team, information sharing platform, or law enforcement.

The CT may at any time order a temporary or complete halt of the test if concerns are raised over damage (or potential damage) to a system. Trusted contacts within the CT positioned at the top of the security incident escalation chain should help to avoid miscommunication and prevent information about the test from being leaked.

4.1.6 Use of code names

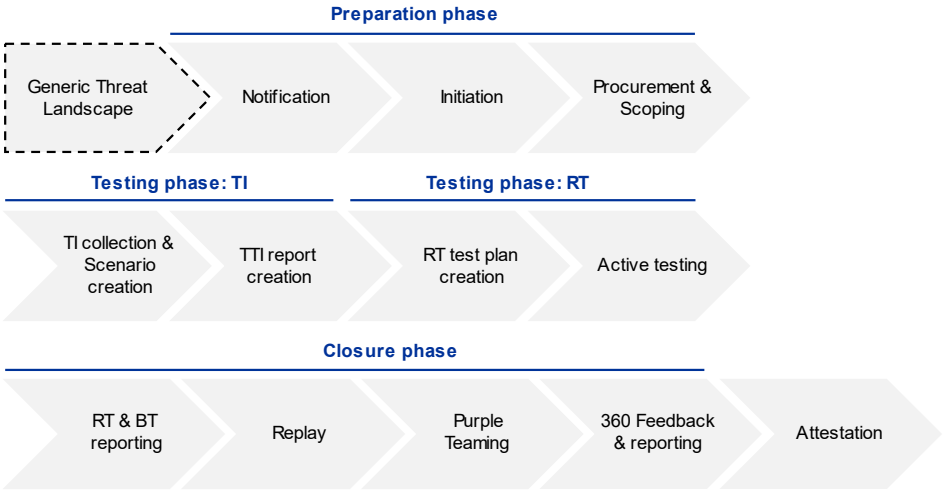
Given the sensitive nature of the tests, and the potentially detailed findings on the weaknesses and vulnerabilities of specific entities, all stakeholders must use code names for the entities being tested, rather than explicitly naming the entity. The entity is responsible for selecting an appropriate code name. Where appropriate, documentation and multilateral communication should only refer to the entity by the commonly agreed code name to protect its identity.

5 Testing process

5.1 High level process overview

The TIBER-EU test process consists of three mandatory phases, namely the preparation phase, the testing phase and the closure phase.

Figure 3
TIBER-EU process



5.2 Generic Threat Landscape

Prior to the preparation phase, a Generic Threat Landscape (GTL) report may be provided by the TCT. The TIBER-EU framework highly recommends that jurisdictions produce or procure a GTL report for the financial sector to complement the more specific TTIR and to provide the basis for scenario development. A GTL report is not mandatory under TIBER-EU but can be a cost-effective tool in each jurisdiction to be used as common ground for all TIP when developing the more specific TTIRs.

The GTL report should elaborate on the specific threat landscape of the country, taking into consideration the geopolitical and criminal threats unique to the jurisdiction. The report should consider key financial market participants and their CIFs, including entities defined in Chapter 2.1, critical third parties, the different threat actors (including their TTPs) targeting these entities, and common vulnerabilities. The GTL report is used to define the specific threat actors targeting the different types of entities; it complements the production of the TTI report and provides the basis for later scenario development. The GTL report should also be used during the preparation phase to guide and inform the initial scoping discussions with the entity.

The GTL report will allow the TIP to:

- translate the information contained in the GTL report into specific strategic, operational and tactical threat intelligence that is relevant to the entity;
- focus on detailed reconnaissance to provide the RTT with bespoke and specific information on the entity, which will in turn allow meaningful attack scenarios to be developed.

The GTL report may be instigated and produced by the TIBER authority, the market (e.g. industry bodies, a consortium of entities or any other financial sector body), or as a joint effort. The report may also be produced by external providers. It is recommended that the report be shared more widely with the financial sector. To provide a broad and realistic overview of the threats to the national (and possibly European) financial sector, the GTL report should be developed using appropriate financial sector threat intelligence expertise. Appropriate threat intelligence expertise can be sourced from entities, national authorities, commercial TIPs, information sharing and analysis centres (ISACs), and market associations. The GTL may be validated and reviewed by the relevant national intelligence agency if possible, and updated on an ongoing basis as new threat actors and TTPs emerge.

6 Preparation phase

6.1 Overview

The preparation phase of a TIBER-EU test starts when the designated contact point of the entity receives a written notification, and the TM starts liaising with the entity. The entity selects a CT and drafts the initiation documents, which include, amongst other information, a high-level project plan as well as communication details. The entity completes an initial risk assessment, as outlined in chapter 4, and takes appropriate measures to mitigate the identified risks. The scope is defined, and the entity procures the TIP and RTT[16].

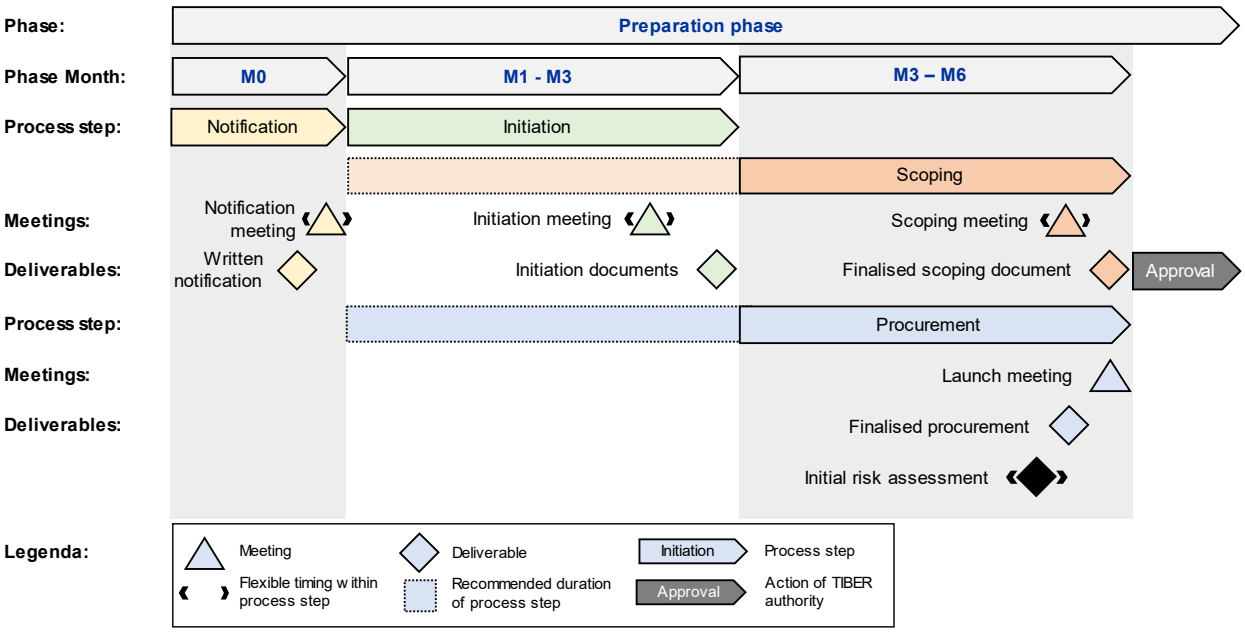
The preparation phase is composed of four process steps, namely (1) notification, (2) initiation, (3) scoping and (4) procurement. The different process steps may be conducted in parallel, and may even start before the notification (e.g. in case of procurement). In the preparation phase, process steps and/or deliverables may be completed earlier than indicated in the figure, or in a different order when feasible.

A process overview of the preparation phase can be found in the figure below.[17]

[16] Procurement is only applicable in the case of external RTT. TIPs are always procured externally.

[17] Note that only the actions of the TIBER authority are included in the figure that have an impact on the timelines of the test. The figure is not an exhaustive overview of all actions to be undertaken by the involved stakeholders.

Figure 3
Preparation phase process overview



6.2 Notification

Following the adoption of the TIBER-EU framework at national or European level, each TIBER authority determines which types of entities are included in the target group of TIBER and, where appropriate, which entities should be appointed to undertake a TIBER test. The TIBER authority, after acquiring the voluntary interest of an entity to be tested, or after having mandated[18] an entity to execute a test in alignment with the respective testing schedule, will send a written notification to the designated contact point of the entity – keeping in mind the confidentiality of the test. The written notification indicates the start date of the preparation phase, being the start of the test. The preparation phase lasts no longer than six months from the starting date highlighted in the notification. Additionally, a TM (as well as at least an alternate) will be assigned to the test by the respective TCT.

After the notification, the TM holds a notification meeting with the entity. The TCT is strongly encouraged to contact the entity as early as possible, ideally well before the above-mentioned written notification. This is to discuss and coordinate when the test will start, also keeping in mind a lengthy procurement and scoping process. Moreover, potential resource and budget constraints need to be anticipated by the entity.

As early as possible but no later than the validation of the initiation documents by the TM, other authorities or entities which might be included in the test should be identified. The TCT responsible for leading the test should inform such other authorities about the test[19]. The tested entity should confidentially inform all the other relevant legal parties to be included in the test, such as subsidiaries, CSPs, etc. The

[18] On the basis of a legislative testing obligation, where the TIBER-EU framework is used as operational guidance on how to comply with these obligations.

[19] E.g. in the case of joint tests under the DORA regulation, see also chapter 3.2.

TM briefs all parties involved on the steps in the TIBER-EU process, documentation, stakeholder roles and responsibilities.

Meeting: Notification

During the notification meeting, the TM will brief the entity on:

- its designation to carry out a mandatory or voluntary test;
- the stakeholder roles and responsibilities;
- the testing process, its elements and deliverables;
- the TCT and CT composition.

Together with the TM, the entity will identify additional entities or legal parties which may have to be involved in the test. The notification meeting takes place with, or shortly after the written notification.

Participants to this meeting are at least: the entity representatives, TM.

Deliverable: Written notification

The TIBER authority sends a written notification to the entity to be tested, marking the start of the test and indicating the requirements to be followed during testing. The tasks of the entity in the preparation phase should be finished within a maximum of six months after the written notification.

6.3 Initiation

The next process step in the preparation phase is the initiation of the project. During this process step, the entity prepares the initiation documents, which include a project charter – comprising a high-level project plan – and communication details and channels to be established. Moreover, the code name for the TIBER test is determined. The information regarding any planned or ongoing test is limited on a need-to-know basis, including the management body of the entity. However, the CT must ensure that the management body of the entity is informed about the progress of the test and its associated risks.

The initiation documents should be delivered to the TM no later than 3 months after the written notification. Since testing is conducted on live production systems, the CT should establish comprehensive risk management measures during the preparation phase to address all potential risks arising from the conduct of the test[20]. The

[20] More information on risk management can be found in chapter 4.

initiation documents will be presented by the CTL in the initiation meeting and are subsequently assessed and validated by the TM.

Meeting: Initiation

During the initiation meeting, the envisioned CTL should brief the TM on:

- the content of the initiation documents;
- the planned composition of the CT;
- contractual considerations regarding procurement;
- Initial efforts undertaken to manage the risks of the test.

The CTL and the TM should discuss the documents, and identify any remaining questions of the CTL or missing information required by the TM. The initiation meeting takes place no later than three months after the notification.

Participants to this meeting are at least: the entity representatives, TM.

Deliverable: Initiation documents

The initiation documents include:

- the project charter, including:
    - a high-level project plan, including the envisioned deadlines of the preparation, testing and closure phase, as well as the deadline for the remediation plan;
    - the name and contact details of the CTL;
    - information on intended use of internal and/or external RTT;
    - secure communication and data transfer channels;
    - the code name for the test;
    - any CIFs the entity operates or shares in another Member State;
    - any CIFs supported by ICT third party service providers.

The CT has to send the initiation documents to the TM no later than 3 months after the written notification.

Available guidance: TIBER-EU Initiation Documents Guidance

Following the validation of the initiation documents by the TM, the CTL sets up the CT. This team comprises a select number of individuals who have critical decision-making capacity, and/or are experts, e.g. cyber, operational and risk specialists, experts from the business areas that support the CIFs, project management etc. Members of the CT are positioned in the entity such that they have access to the top of the security incident escalation chain. The composition of the CT can be flexible, depending on the specific structure and organisational set-up of the entity. The TM validates the initial composition of the CT, as well as any subsequent changes to it, and informs the entity of its validation. The CTL makes sure that the CT is aware of the TIBER test, the need for secrecy and the process the CT should go through in case the BT detects and escalates a TIBER-related incident.

6.4 Scoping

During the scoping process step, the tested entity must complete a TIBER-EU Scope Specification document (SSD) listing the CIFs, the systems and services underpinning each CIF, as well as the flags to be captured for each system.

The key objective of the scoping process is for the involved entities to select, and for the TM to validate, the CIFs to be included in the test. A CIF is defined as[21]:

"*a function, the disruption of which would materially impair the financial performance of a financial entity, or the soundness or continuity of its services and activities, or the discontinued, defective or failed performance of that function would materially impair the continuing compliance of a financial entity with the conditions and obligations of its authorisation, or with its other obligations under applicable financial services law*".

Entities may conduct a business impact analysis defining the CIFs as part of their standard business continuity management or operational risk management practices, which may be used as input. CIFs need to be identified on a comparatively high level and might be aggregated to more abstract CIFs. For large and complex entities with numerous CIFs, it may not be feasible to conduct an effective test with all CIFs in the scope of a single test. In this case, there needs to be a rationale on why certain CIFs are not included in the test, which is clearly outlined within the SSD. As a rule of thumb, taking into consideration different levels of abstraction that entities may use in identifying CIFs, and without prejudice to regulatory requirements, a maximum number of 10 CIFs per tested entity is adequate. Also, it is important to note that even though CIFs are scoped within a test, this does not mean that all these CIFs are actively targeted in the testing phase, as this is contingent on the threat intelligence and ultimately the attack scenarios and attack path of the RTT. To identify appropriate CIFs, and subject to availability in the respective jurisdiction, the entity may also refer to a GTL report for examples and to further contextualise its business and the threats it faces.

Entities across the sector support and deliver these CIFs in different ways via their own internal processes, which are in turn underpinned by critical technological systems. It is these critical technological systems, processes, and the people operating them that are the focus of TIBER-EU tests. In most cases, this will also include the systems, people and business processes underpinning the entity's CIFs that are outsourced to third-party service providers. The entity may decide at its discretion to include additional non-critical components in the scope, provided the inclusion does not negatively affect the testing of the CIFs, e.g. pre-production, testing, backup and recovery systems.

For each system in scope, the CT should set at least one "flag" to be captured during the test. A flag is essentially the objective that the RTT must strive to achieve during the test, e.g. compromising the confidentiality, integrity, or availability of the target system. To realistically simulate threat actor behaviour, the entire ICT infrastructure of the entity may be used as "entry point" or "pivot point" to access the systems underpinning the CIFs. In case the ICT infrastructure of the entity is (partially) outsourced, it is recommended for the entity to ensure that ICT service contracts

[21] As defined under DORA, article 3(22).

allow for testing on the supplier infrastructure, or to include such clauses in future contracts.

The CT shall organise a scoping meeting to discuss the scope of the test with the TM, as well as the TIP and RTT (if already procured) and shall incorporate any received feedback. If applicable, feedback on the test scope might also be provided by other TIBER authorities, the entity's supervisors/overseers. As a minimum, the CT should discuss the flags with the TM, who must be involved throughout the scoping process.

The SSD must be delivered by the entity to the TM within six months from the written notification and should be approved by the management body of the entity. The TIBER authority validates the SSD and should inform the CTL about the validation. Once contracted, the CT shall share the SSD with the TIP and RTT.

Meeting: Scoping

During the scoping meeting, the CT and TCT, TM (and TIP/RTT if already procured) should:

- discuss the scope of the test, including feedback by the TCT and/or supervisor (where applicable);
- update the TIP and RTT on the scope (this might be done afterwards if the providers are not yet procured);
- present the updated risk management measures and documentation.

The scoping meeting takes place after the initiation meeting, but no later than six months after the written notification.

Participants to this meeting are: the CTL, CT, TM, (TIP and RTT).

Deliverable: Scope Specification Document

The CT will deliver a SSD, setting out:

- the CIFs identified by the entity;
- for each CIF in scope of the test:
  - the reason why the CIF is included;
  - the ICT system(s) supporting the CIF; stating a) whether this system is supported by ICT third-party providers and to which one, b) the jurisdictions in which the ICT system is used; and c) a high-level description of the preliminary flag(s) indicating which security aspect of confidentiality, integrity, and availability is covered by each flag;
  - If identified CIFs are not included in the scope of the test, the CT should provide an explanation of why the CIFs are not included in scope.

The SSD should be approved by the management body of the entity, and delivered to the TM within six months after receiving the written notification.

Available guidance: TIBER-EU Scope Specification Document Guidance

Prior to the testing phase, the CT should consult the TM on the risk assessment and risk management measures, as outlined in chapter 4. The CT shall review the risk assessment and risk management measures in case the TM assesses that they do not adequately address the risk of the TIBER test. Moreover, the CTL should regularly assess the risks and the related mitigation measures throughout the test.

6.5 Procurement

Owing to the sensitive nature of the TIBER-EU test, and the fact that it is carried out on live production systems, it is critical that the TIP and RTT possess the highest levels of skills, capabilities and qualifications. The entity must therefore select an external TIP and external (or under certain circumstances internal) RTT with the requisite skills and experience to perform the test.

To ensure that the TIP/RTT meet the appropriate standards for conducting such a test, the entity should conduct its own due diligence as part of its procurement process and existing risk management practices to ensure that the procured TIP and RTT meet the minimum requirements set out in the GSPP. These are deliberately stringent requirements intended to mitigate the risk of tests being conducted by inexperienced personnel, which could have an adverse impact on the operational stability of the tested entity or the execution of the test. Regarding the relevant certifications for the RTT and TIP, the providers send copies of certifications to the CT[22]. Responsibility for ensuring that the appropriate TIP/RTT are selected lies solely with the entity. The CT should document its assessment of compliance and provide evidence of compliance to the TM. The CT does not proceed with contracting

[22] These certifications may e.g. be sent to the CT as part of the respective CVs.

the selected TIP/RTT where the TM assesses that the selected providers do not ensure compliance.

In exceptional circumstances, the entity could end up having to contract testers that do not meet the minimum requirements for providers. In such a case, the entity is required to adopt appropriate measures mitigating the risks relating to the lack of compliance with the requirements, and provide evidence of these measures to the TM. If applicable, the above circumstances will be documented in the test attestation.

Once the procurement process has been completed and all relevant contractual arrangements are in place, the CTL should update the project plan – in consultation with the TM, including the final schedule of process steps, deliverables and meetings to be held between the entity, TIP/RTT and TM. The CTL should share all relevant parts of the initiation documents, such as the project plan, secure communication and data exchange channels as well as the code name with all the relevant stakeholders.

The TM may allow a degree of flexibility to the entity on the timing of the procurement, as the process may differ across jurisdictions. However, the procurement of providers must be finalised before the start of the testing phase. The entity should, as early as possible, start the procurement process to ensure that there are no bottlenecks or delays in the overall testing process.

After the contracts with the TIP and the RTT have been signed, the CT organsises a launch meeting, to officially onboard the TIP/RTT to the test and to introduce them to the testing process, project plan, rules of engagement and stakeholder expectations. This meeting includes the TM and, where applicable, representatives from other TIBER authorities.

Meeting: Launch

The launch meeting should involve all the relevant stakeholders (including the TM, CT and TIP/RTT). During this meeting, the following actions are performed:

- the TIP/RTT are officially onboarded;
- the CT composition and project plan are presented;
- the presentation of the scope, if feasible;
- the test process, the rules of engagement and established communication details and channels are presented;
- all stakeholders discuss their expectations and their cooperation.

The launch meeting is held when the procurement is finalised, no later than six months after the written notification.

Participants to this meeting are, at least: the CT, TM, TIP & RTT.

Deliverable: Procurement completed

The CT has completed procurement of the TIP and RTT and onboarded them to the test, prior to the start of the testing phase. The compliance of the providers with the applicable requirements and criteria has been assessed by the CT and TM.

Available guidance: **TIBER-EU Guidance for Service Provider Procurement**

7 Testing phase: threat intelligence and scenarios

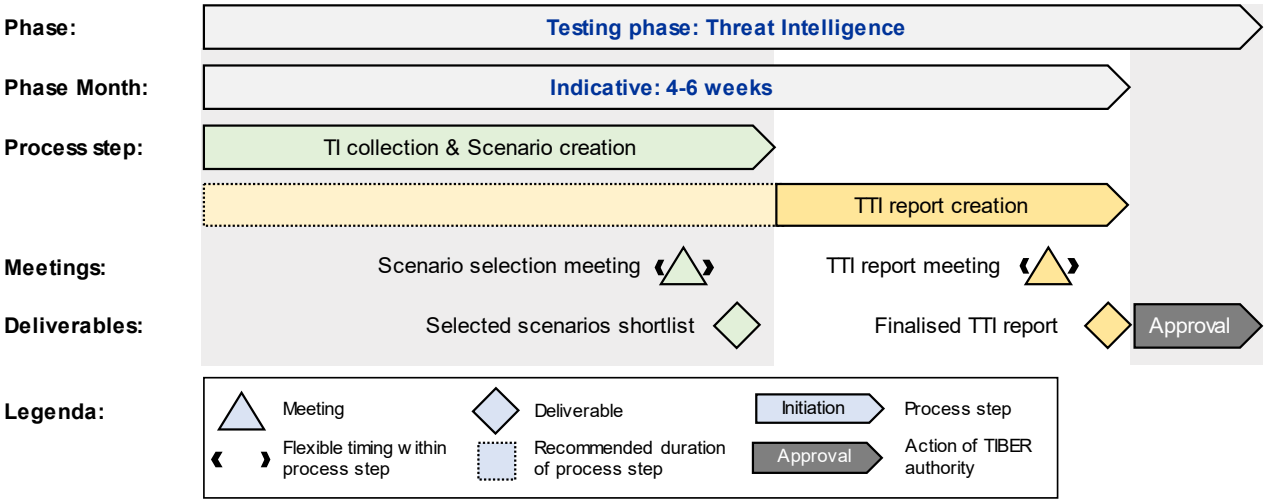
7.1 Overview

Once all activities in the preparation phase are concluded, the testing phase officially starts with the threat intelligence (TI) component. The threat intelligence phase consists of two process steps, namely i) TI collection and scenario creation and ii) creation of the Targeted Threat Intelligence Report (TTIR). An overview of the threat intelligence phase can be found in figure 4 below[23]. Threat intelligence-based scenarios mimicking real-life cyber adversaries are essential to the realism and success of testing activities.

During TI collection and scenario creation, the TIP collects, analyses, and disseminates tailored intelligence relating to two key areas of interest:

- target intelligence: information on potential attack surfaces and exposures across the entity;
- threat intelligence: information on relevant threat actors and probable threat scenarios.

Figure 4
Testing phase: Threat Intelligence process overview



Based on this information the TIP will develop a broad set of high-level scenarios, which are tailored to the tested entity and from which test scenarios will be selected during the scenario selection meeting. The draft high-level scenarios should vary

[23] The figure only includes the actions of the TIBER authority that have an impact on the timelines of the test. The figure is not an exhaustive overview of all actions to be undertaken by the involved stakeholders.

regarding the included threat actors and TTPs – and together cover all CIFs in scope.

Additionally, the TIP drafts a dedicated TTIR, outlining the entity-tailored threat landscape as well as further elaborating on the selected scenarios. When the TTIR is in its final stage, a TTIR meeting is held to discuss the reported findings. The TTIR, after approval of the TM, will form the basis for the RTTP creation in the testing phase.

7.2 Key considerations for the Threat Intelligence Provider

7.2.1 Sources of collected TI

For the TIBER-EU framework to work effectively, it is critical that the TTI process and subsequent deliverables meet the highest standards. Intelligence encompasses not only the technical details of the attack but also an understanding of the TTPs behind the attack and the threat actors themselves, including their intent, capability and modus operandi.

The TIP is expected to:

- engage with the entity to obtain useful context for conducting the threat analysis. Although the CT may not always be allowed to share sensitive details with the TIP, it should still be possible to learn about the entity both through engagement with the key stakeholders and by gathering evidence of previous breaches through public sources;
- be able to adequately cooperate with the internal threat intelligence capabilities (Cyber Threat Intelligence; CTI) of the testing entity. Even though there needs to be an external provider – and thus an outside perspective on the entity – cooperation with the internal CTI team may reap many benefits, among which efficiency and a deeper analysis of the entities' environment;
- use a broad range of sources, e.g. internet services, a mixture of public and private fora and a range of media types such as internet relay chats, email and video. The number of items in any given source type is a useful means of measuring the provider's TI collection capabilities. However, volume can at times undermine quality, and it is expected that the collection of sources be balanced against the ability of the TIP to refine, analyse and discard sources in an accurate manner;
- have a depth of sources. TIPs collecting intelligence may only use surface content from a given source, but it is also important to know that all the content of a given source can be incorporated when there is an appropriate and lawful opportunity to do so. It is therefore expected that a TIP can provide the option to acquire data at scale and in its original context;
- only use TI gathering techniques that do not (risk to) compromise the secrecy of the test. In case of doubt as to whether certain techniques may be used, the TIP should liaise with the CT, TM and RTT;

- have adequate language support. Languages play an important role in providing CTI. Cyber threats are a global phenomenon, and a TIP that offers little linguistic coverage of online threats will potentially miss a significant proportion of relevant information;
- be able to use a variety of methods in intelligence gathering, for example OSINT (which is derived overtly from publicly available sources) and HUMINT (human intelligence, which is derived overtly or covertly from human sources);
- demonstrate strong ethical behaviour, and cooperate with the RTT in a flexible and transparent manner, when required, in the testing process.

7.2.2 Collected threat intelligence

The TIBER-EU process is designed to create realistic threat scenarios describing attacks against an entity. These scenarios can be used by the RTT to guide its intelligence-led red team test. The scenarios are based on available evidence of real-world threat actors, combined with OSINT data on the entity as well as some knowledge of the CIFs that form the scope and target of the test.

While this approach is highly valuable, real-world threat actors may have months to prepare an attack. In addition, while TIPs are constrained by limitations on the time and resources available, and by moral, ethical and legal boundaries, real-world threat actors are free of such constraints. This difference can cause difficulties when attempting to design realistic scenarios that can be executed within those boundaries, as sensitive data about the target, e.g. knowledge about the internal network, is often hard to gain using morally, ethically or legally justifiable techniques.

Similar constraints apply to CIFs, which are internal to the entity and typically do not have a large footprint in the public domain. They also apply to the systems that underpin CIFs, whether these are bespoke internal systems or external systems that span multiple organisations with a common connecting infrastructure.

Therefore, to make intelligence gathering as efficient as possible given the time and resource constraints, and to ensure the intelligence is relevant to the scope and the entity's business, the TIP should seek from the entity and be provided with:

- a business and technical overview of each CIF-supporting system in scope;
- the current threat assessment and/or threat register;
- examples of recent attacks on the entity or its environment;
- previous TTIR used in TIBER tests, if relevant and deemed feasible by the entity.

The entity should provide the above information to the TIP to facilitate scenario development. In cases where the entity has an internal CTI function, the TIP could liaise with it and gather relevant information that will help inform the TTIR. Prior to liaising with the internal CTI capability of the testing entity with the TIP, the CTL should take appropriate measures to safeguard the confidentiality of the test.

Finally, in cases where the respective jurisdiction(s) has/have produced a GTL report, the TIP should use this as a basis for producing the TTIR, focusing on how to

contextualise the threat landscape of the country, the different threat actors and the common vulnerabilities to the specificities of the entity.

7.2.3 Collected target intelligence

To identify targets, the TIP should carry out a broad exercise of the kind typically undertaken by threat actors as they prepare for their attack from outside the network. The objective is to form a detailed preliminary picture of the entity and its weak points from the attacker's perspective. This will enable the TI to be put into context and will contribute to the development of the threat scenarios in the TTIR. Part of this information should be provided by the entity using the TIBER-EU Targeted Threat Intelligence Report Guidance.

The output of this activity is the identification, on a CIF-focused, system-by-system basis, of the attack surfaces of people, processes and technologies relating to the entity, and its global digital footprint. This includes information that is intentionally published by the entity and internal information that has been unintentionally leaked. Such information could be customer data, confidential material or other information that could prove to be a useful resource for an attacker.

The TTI gathering represents a valuable input and is a core element of the TTI report, where it is used to tailor the threat profile and scenarios. By revealing some of the entity's attack surfaces and identifying initial targets, it also serves as a valuable input into the RTT's deeper and more focused targeting activities.

7.3 Scenario creation

In this process step, a broad set of scenarios is created by the TIP and presented to the stakeholders during the selection meeting. The scenarios should be based on intelligence acquired during the target identification process and should present a credible picture of the entity's cyber threat landscape, i.e. threat intelligence-based and specifically tailored to the entity's business environment, including its key threats and detailed profiles of the threats and actors with the highest scores. Based on this set, the final scenarios used for testing will be selected.

While the threat scenarios are fictional, they should be based on real-life examples of cyber-attacks including the motivations of the attackers, their objectives, and the methods they employ to meet them. By focusing on what is realistic rather than theoretically possible, the scenario identification supports the RTT in justifying the approach it plans to take.

In addition to threat-led scenarios, the TIP may develop other types of scenarios. For example, in cases where the use of conventional TTPs may not be successful in achieving a flag. To emulate a real-life attacker in such a case, the TIP could deploy creative and innovative TTPs. Along these lines, the TIP can leverage their full range of professional knowledge, research, expertise and tools to build forward-looking scenarios based on TTPs that have not yet been seen but are expected in the future. Such scenarios may include hybrid, novel TTPs and "out of the box" elements. Also, a certain scenario might be of great relevance to a tested entity, even though it is not threat-led.

A maximum of one scenario (out of the three selected scenarios) per TIBER test may be non-threat-led, allowing for the investigation of future or otherwise relevant attack vectors. Such a scenario is referred to as scenario-X. If no scenario-X is specified during the threat intelligence phase, a maximum of one scenario may be transformed into a scenario-X during the active testing phase, after agreement of the TM, CT and RTT.

In case of a multi-party test involving an ICT third party provider, at least one of the selected scenarios should cover the ICT third party providers' systems, processes and technologies supporting the CIFs of the entities in scope.

Based on the information of the collected TI and the selected scenarios, the CT must start to plan for the potential use of leg-ups. Leg-ups are network and system accesses and/or devices that may be needed by the RTT in their execution of the scenarios. Leg-ups could also include additional information on target systems and technology. The RTT are invited to offer their expert view on what kind of leg-ups would be more suitable. It should be noted that actions such as directly providing access to the flags and/or disabling security controls should not be proposed as leg-ups[24].

Meeting: Scenario selection

During the scenario selection meeting, the TIP introduces a broad set of realistic attack scenarios, based on the collected entity-tailored TI and an evaluation of every CIF in scope of the test. The scenario selection meeting is held when the longlist with scenarios is ready to be shared and discussed.

Participants to this meeting are: the CT, TM, TIP & RTT

Deliverable: Scenarios created and selected

The CTL selects/adapts three or more scenarios to be followed during testing, based on:

- the recommendation of the TIP, taking into account the threat-led nature of the scenarios;
- the input provided by the TM;
- the feasibility of the proposed scenarios for execution, based on the expert judgement of the RTT;
- strategic criteria (e.g. regarding scenarios of past tests, the need for leg-ups);
- the size, complexity and overall risk profile of the entity and the nature, scale and complexity of its services, activities and operations.

Available guidance: TIBER-EU Targeted Threat Intelligence Report Guidance

[24] More information on leg-ups can be found in the TIBER-EU Control Team Guidance.

7.4 Targeted Threat Intelligence Report creation

This process step focuses on the finalisation of the TTIR, which is a bespoke, report for the entity being tested. The TTIR creation process step builds on the initial TI work completed during the TI collection and scenario-creation process step. Responsibility for the development and production of the TTIR lies with the TIP. After the scenario selection meeting, the RTT are more involved, absorbing the contents of the TTIR and preparing to integrate the attack scenarios into a RTTP. To enrich the TTIR, the RTT are encouraged to give feedback during the final stage of the TTI process.

Two elements are particularly relevant in order to provide a firm TI basis for the RTTP:

- tailored scenarios, which will support the formulation of a realistic and effective RTTP;
- threat actor goals, motivations and TTPS, which will help steer the RTT in its attempt to capture the flags;

In addition, based on the TTI report, the CT and TM may opt to update or modify the flags. The CT should update their risk management controls after the receipt of the TTI report, where applicable.

After finalisation, the CT should send the TTI report to the TM for approval, who will notify the CTL accordingly.

Meeting: TTI Report

During the TTIR meeting, the TIP should present:

- the collected target intelligence;
- the selected and elaborated scenarios for testing – in detail;
- the draft TTIR.

All stakeholders should provide feedback on and discuss the report, identifying potential aspects to be added/changed. If necessary, flags might be updated in the light of the report data, and potential leg-ups should be explained. The TTIR meeting is held as soon as the report is in its final stage.

Participants to this meeting are, at least: the CT, TM, TIP & RTT

Deliverable: TTI Report

The TIP delivers a dedicated TTI report, containing the elements as described in the TIBER-EU Guidance for the TTI report, outlining the entity-tailored threat landscape as well as describing the selected scenarios in detail. The report shall contain at least the following elements:

1. The overall scope of the intelligence research, including the:
    a. CIFs in scope and their geographical location;
    b. official EU language(s) in use;
    c. relevant ICT third party service providers;
    d. period of time over which the research is gathered.

2. An overall assessment of what concrete, actionable intelligence can be found about the entity, such as:
    a. employee usernames and passwords;
    b. look-alike domains which can be mistaken for official domains of the entity;
    c. technical reconnaissance: vulnerable and/or exploitable software, systems and technologies;
    d. information posted by employees on social media, related to the entity, which might be used for the purposes of an attack;
    e. information for sale on the dark web;
    f. any other relevant information available on the internet or public networks;
    g. where relevant, physical targeting information, including ways of access to the premises of the financial entity.

Deliverable: TTI report

3. Threat intelligence analysis considering the general threat landscape and the particular situation of the entity, including at least the:
   a. geopolitical environment;
   b. economic environment;
   c. technological trends and any other trends related to the activities in the financial services sector.

4. Threat profiles of the malicious actors (specific individual/group or generic class) that may target the entity, including the systems of the entity that malicious actors are most likely to compromise or target, the possible motivation, intent and rationale for the potential targeting and the possible modus operandi of the attackers.

5. Threat scenarios: at least three end-to-end threat scenarios for the threat profiles identified in accordance with point 4, who exhibit the highest threat severity scores. The threat scenarios shall describe the end-to-end attack path and shall include, at least:

   a. one scenario that includes, but is not limited to, compromised service availability;
   b. one scenario that includes, but is not limited to, compromised data integrity;
   c. one scenario that includes, but is not limited to, compromised information confidentiality;
   d. Optionally: a scenario-X.

Available guidance: **TIBER-EU Targeted Threat Intelligence Report Guidance**

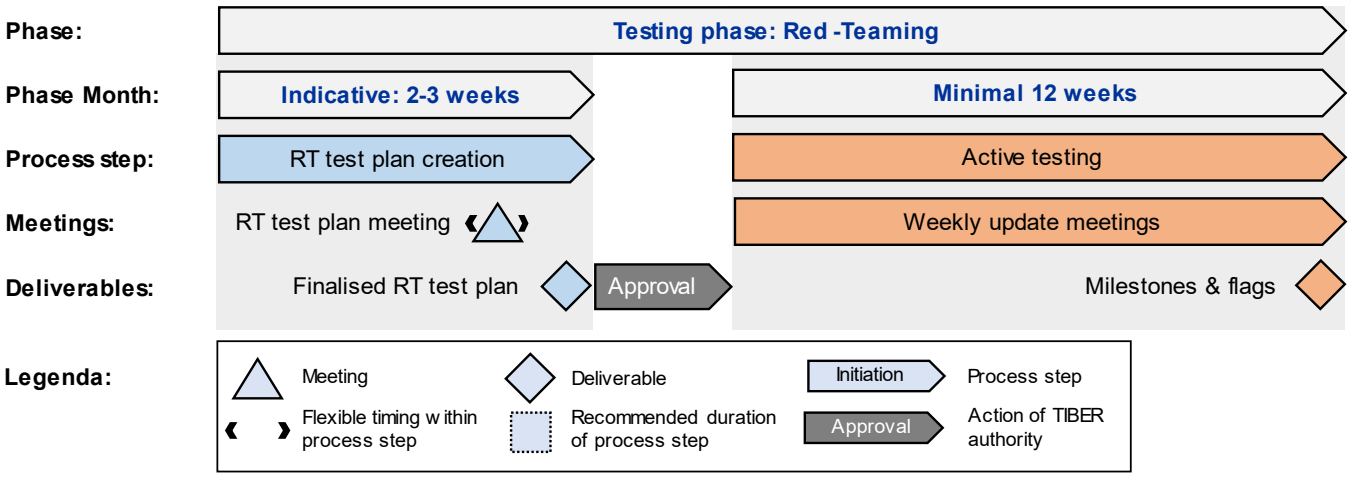
8 Testing phase: red team testing

8.1 Overview

Following the approval of the TTIR by the TM, the RT activities move into focus. During the red-teaming phase, the RTT plans and executes a TIBER test on the basis of the respective selected scenarios for the target systems and services that underpin the selected CIFs in scope. A process overview of the red-teaming phase can be found in the figure below[25].

The red-teaming phase consists of two separate process steps, namely (1) the Red Team Test Plan (RTTP) creation and (2) the active testing. The TTIR forms the basis of the RTTP. When the RTTP is in its final stage, the stakeholders hold a RTTP meeting, after which the plan is approved. After approval of the test plan by the CT and the TM, the active testing process step starts. During the active testing, the RTT aim to reach all the flags, as defined in the test plan.

Figure 5
Testing phase: Red-Teaming process overview



8.2 Key considerations for the Red Team Testers

8.2.1 Deploying a range of TTPs during testing

The RTT should deploy a range of TTPs during the test. The following list is just one example of a testing methodology that the RTT may use.

Reconnaissance – The first phase in a red team test is focused on collecting as much information as possible about the target. Reconnaissance is one of the critical

[25] Note that only the actions of the TIBER authority are included in the figure that have an impact on the timelines of the test. The figure is not an exhaustive overview of all actions to be undertaken by the involved stakeholders.

steps, and can lead to significant discovery about the target's people, processes, technology, surroundings, and environment. This step may also involve building or acquiring specific tools for the engagement.

Weaponisation – By thoroughly analysing information gathered about the infrastructure, facilities and employees, the RTT begin to form a picture of the target and its primary operations. Effective weaponization involves preparation for the operations specific to the targets.

Delivery – This marks the active launch of the full operation. The RTT begin to carry out the actions intended to reach the targets or flags, such as social engineering, analysing cyber vulnerabilities, planting hardware Trojans for remote network persistence, etc. One of the most important objectives is to identify the best opportunities for exploitation.

Exploitation – During exploitation, the RTT's goal is to "break in", i.e. to compromise servers/apps/networks and exploit target staff through social engineering. The exploitation stage paves the way for the control and movement phase.

Control and movement – Once a successful compromise has been performed, attempts to move from initial compromised systems to further vulnerable or high-value systems will be made. For example, this may consist of "hopping" between internal systems, continually reusing any increased access obtained in order to eventually compromise agreed target systems.

Actions on target – This entails gaining further access to compromised systems and acquiring access to previously agreed target information and data. At this point, the RTT aim to complete the test and achieve the objectives and capture the flags.

8.2.2 Grey-boxing and leg-ups

The TIBER-EU process is designed to create realistic scenarios mimicking possible future attacks against the entity. Real-world threat actors may have months to prepare an attack. They are also able to operate freely without the constraints that TIP/RTT face, such those on time and resources – not to mention the moral, ethical and legal boundaries. This difference can cause challenges when attempting to create realistic scenarios, as knowledge about the internal network is often the hardest to gain using morally, ethically or legally justified techniques.

Similar constraints apply to the systems underpinning the CIFs, which typically do not have a large footprint on the public internet. Whether they are internal bespoke systems or external systems that span multiple organisations with a common connecting infrastructure, the RTT knowledge of the functioning of these systems may be limited in comparison with that of attackers who have the capacity and time to study them extensively.

Therefore, to facilitate a more effective and efficient test, the entity may deliver additional information to the RTT on the scenarios chosen, including on the people, processes and systems targeted in the scenario. This information may give the RTT further insights and allow a better use of time. However, it is up to the entity to provide this additional information and the underlying level of detail at its discretion.

If the entity provides additional information, the TIBER-EU test will reflect a “grey box” testing approach in contrast with the “black box” approach. Experience shows that the more relevant information an entity gives to the TIP/RTT, the more the participating entity will gain from the test. However, it should be evident that the information given to the TIP could have been obtained by an advanced attacker with more time and unhindered by moral, ethical and legal constraints.

During the testing phase, the RTT may be unable to progress to the next stage owing to time constraints or because the entity has been successful in protecting itself. In such scenarios, the RTT, with approval from the CT and TM, may be given a leg-up, for instance where the entity essentially gives the RTT access to its system, internal network, etc. to continue with the test and focus on the next flag/target. The leg-ups are usually, but not limited to, system or network access, information on targets etc. Should this happen, then the leg-up should be duly logged. This ensures that maximum benefit is derived by all stakeholders from a time-limited test. It is important that the CT, in consultation with the TM, stands ready to provide a leg-up and not unduly delays the test.

In addition to the information provided by the entity, the role of the TIP can be enhanced during the testing phase. For the test to succeed, the TIP can provide ongoing TI to the RTT during the test, which may provide more useful reconnaissance and more insight on how to achieve the targets. In real life, the attacker can leverage TI while attempting to compromise an entity. Allowing a fluid relationship between the TIP and RTT during the test may add greater value to the test. Where TIP and RTT decide to work more closely during the test, the working arrangements and information sharing arrangements must be agreed between the two parties.

8.3 Red Team Test Plan creation

In this process step, the RTT develops and integrates the attack scenarios into a RTTP, leveraging on the scenarios included in the TTIR[26].

The RTT should align its test objectives with the goals of each of the actors, map these to the CIF-supporting systems, and produce credible real-life attack scenarios for the test. The attack scenarios are designed to provide background to the tradecraft employed by each threat to conduct a successful attack. The RTT should therefore adapt its attack methodology to replicate the real-life attack scenarios.

The RTT could also add some elements which test the response of the entity, including evidence on whether the compromise action would be immediately detected or could have a fair chance of succeeding.

Performing any sort of red team test always carries a level of risk to the target system and the business information associated with it. Risks to the entity, such as degradation of service or disclosure of sensitive information, need to be kept to an absolute minimum. The RTT should therefore include an appropriate plan to assist the entity in managing these risks.

The attack scenarios are written from the attacker’s point of view and should define the concrete targets to be reached (i.e. the flags to be captured). The RTT should

[26] More information can be found in the TIBER-EU Red Team Test Plan Guidance.

indicate various creative options in each of the attack phases based on various TTPs used by advanced attackers to anticipate changing circumstances or in case the first option does not work. The scenario writing is a creative process. The TTPs do not simply mimic scenarios seen in the past but combine the techniques of the various relevant threat actors.

Scenarios to be tested may also include the usage of TTPs which look to breach the physical security of the entity to gain access to the network or plant a device. However, if such a method is used, appropriate safeguards (e.g. formal consent by the entity) should be in place and no legal boundaries should be crossed. The risk of detection from each scenario must also be taken into consideration when drafting the test's timeline and setting up the order of scenario execution.

The output of this activity is the final RTTP, including the attack scenarios to be followed and the risk management controls that will be applied to ensure that the test is conducted in a controlled manner, including the frequency of test progress reports with the CT and the TM.

Once the RTTP is in its final phase, the RTT, TM, CT, and the TIP, where appropriate, come together to discuss it during the RTTP meeting. The RTT explain their envisioned approach to reach the flags, as well as the technical measures they will take for doing so, and the leg-ups they might require at certain points.

The CT and the TM approve the final RTTP – and any subsequent changes to it – which should include, if any, the feedback received during the meeting.

Meeting: RTTP

During the RTTP meeting the RTT should present:

- the planned attack steps for each end-to-end scenario, including detailed flags and expected leg-ups;
- time planning for each scenario;
- dedicated milestones;
- escalation contacts and procedures;
- rules of engagement and reporting agreements;
- risk management measures taken by the RTT.

All stakeholders should provide feedback on and discuss the test plan, identifying potential aspects to be added/changed.

Participants to this meeting are at least: CT, TM, RTT, TIP (where appropriate).

Deliverable: RTTP

The RTT delivers a dedicated RTTP before the start of active testing, according to the information included in the TIBER-EU Guidance for Red Team Test Plan. The RTTP should contain at least:

1. the communication channels and procedures;
2. test progress reporting procedures and frequency;
3. the TTPs allowed and forbidden for use in the attack including ethical boundaries for social engineering, and how the privacy of involved parties is being safeguarded;
4. risk-management measures to be followed by the testers;
5. a description for each scenario, including:
    a. the simulated threat actor;
    b. their intent, motivation and goals;
    c. the target function(s) and the supporting ICT system or systems;
    d. the targeted confidentiality, integrity, availability and authenticity aspects;
    e. the flags;
6. a detailed description of each expected attack path, including pre-requisites and possible leg-ups to be provided by the CT, including deadlines for their provision and potential usage;
7. the scheduling of red teaming activities, including time planning for the execution of each scenario, at a minimum split according to the three phases a tester takes throughout the testing phase, respectively entering financial entities' ICT systems, moving through the ICT systems and ultimately executing actions on objectives and eventually extracting itself from the ICT systems (in, through and out phases);
8. any particularities of the entities' infrastructure to be considered during testing;
9. if any, additional information or other resources necessary to the testers for executing the scenarios.

Available guidance: **TIBER-EU Red Team Test Plan Guidance**

Upon finalisation of the RTTP, the CT must update its risk management controls and prepare specific leg-ups to the RTT, by being ready to execute all necessary processes and procedures without raising alarm and causing delay.

8.4 Active testing

Once the RTTP is approved by the CT and TM, the RTT should initiate the active execution of the test. Any changes to the RTTP subsequent to its approval must be approved by the CT and TM. The attack scenarios are not a prescriptive playbook

which must be followed precisely during the test. If obstacles occur, the RTT should show its creativity (as advanced attackers would) to develop alternative ways to reach the test objective or flag.

A minimum of 12 weeks must be allocated to active testing, to allow the RTT to conduct a realistic and comprehensive test in which all attack phases are executed – and the flags can be reached. Within this time frame, attack scenarios can be executed in parallel or in sequence. When executing scenarios in parallel, the RTT still needs to complete all the scenarios' in-through-out phases.

The RTT is constrained by the time and resources available as well as by moral, ethical and legal boundaries. It is therefore possible that the RTT may require occasional leg-ups in addition to those laid out in the test plan to help the RTT progress. All leg-ups are to be provided by the CT, and approved by both the CT and the TM.

During the execution of the test, it can happen that a staff member of the entity or its ICT third-party service provider irrevocably detects the RTT via its activities. In such cases, the CT should propose and submit measures allowing to continue the test to the TM for its validation whilst ensuring that the secrecy of the test is upheld. Other cases may include the discovery of an actual compromise or any other exceptional circumstances triggering risks of impact on data, damage to assets, disruption to CIFs, services or operations. Under such exceptional circumstances, after consultation with the TM, the CTL may suspend the test as needed to thereby facilitate delays or employ other changes to continue the test and maximise its learning experience.

In case a critical vulnerability is discovered during this phase, the CT may also initiate remediation actions, based on technical feedback provided by the RTT, and in close consultation with the TM, while ensuring the minimum possible impact to the testing activities and confidentiality.

As a last resort, if continuation of the test is not otherwise possible, and insofar possible strictly within a scenario, testing activities can be continued as a limited PT exercise during the testing phase – subject to prior validation of the TM. The duration of the limited PT exercise counts towards the 12-week minimum duration of the active red team testing phase[27].

Irrespective of the methodology used by the RTT, the test should be conducted in a controlled manner, taking a stage-by-stage approach, and in a way that minimises risks to the entity and its CIFs. All of the RTT actions should be logged: for the replay exercise with the BT, as evidence for the RTTR, and for future reference.

[27] More information can be found in the TIBER-EU Purple Teaming Guidance.

Meeting: Weekly updates

During active testing, the CT should organise at least weekly meetings for the RTT to update the CT and TM on the testing progress. For example, the activities conducted in the past week along with activities expected in the upcoming week. The TIP may be involved for consultation if requested by the CT.

In addition to the weekly updates, it is highly recommended for the RTT to arrange daily meetings and ad-hoc (secure) communication involving the CT and the TM. Here, the focus should be on activities of the immediate past and short-term planned actions, especially during critical testing phases.

Participants to these meetings are: the CT, TM, RTT (TIP if requested).

Deliverable: Milestones & Flags

During active testing, the goal of the RTT is to reach all the flags. When a milestone deadline is reached, the CT should (if necessary) provide the respective leg-up, as specified in the RTTP, to the RTT for efficient continuation of the test.

The CT, TIP, RTT and TM should agree on the concrete end of the active RT phase. Following the end of the active RT phase, the CTL will inform the BT that a test was conducted. After the test, the RTT and TIP should carry out restoration procedures, in order to safeguard the integrity of the tested entity's environment. These restoration procedures should be planned and coordinated with the CT and BT, and ideally not occur before the replay and PT exercise in the closure phase. The procedures include the deletion of information related to passwords, credentials (or changing them) and other (secret) keys compromised during the test. It also entails the restoration and deletion of compromised secure communication channels to the entity, secure collection, storage, management and disposal of collected data.

Technical restoration procedures should include;

- command and control deactivation;
- scope and date kill switches;
- removal of backdoors and other malware;
- potential breach notification;
- procedures for future back-up restauration which may contain malware or tools installed during the test;
- monitoring of the BT activities and information to the CT of any possible detections.

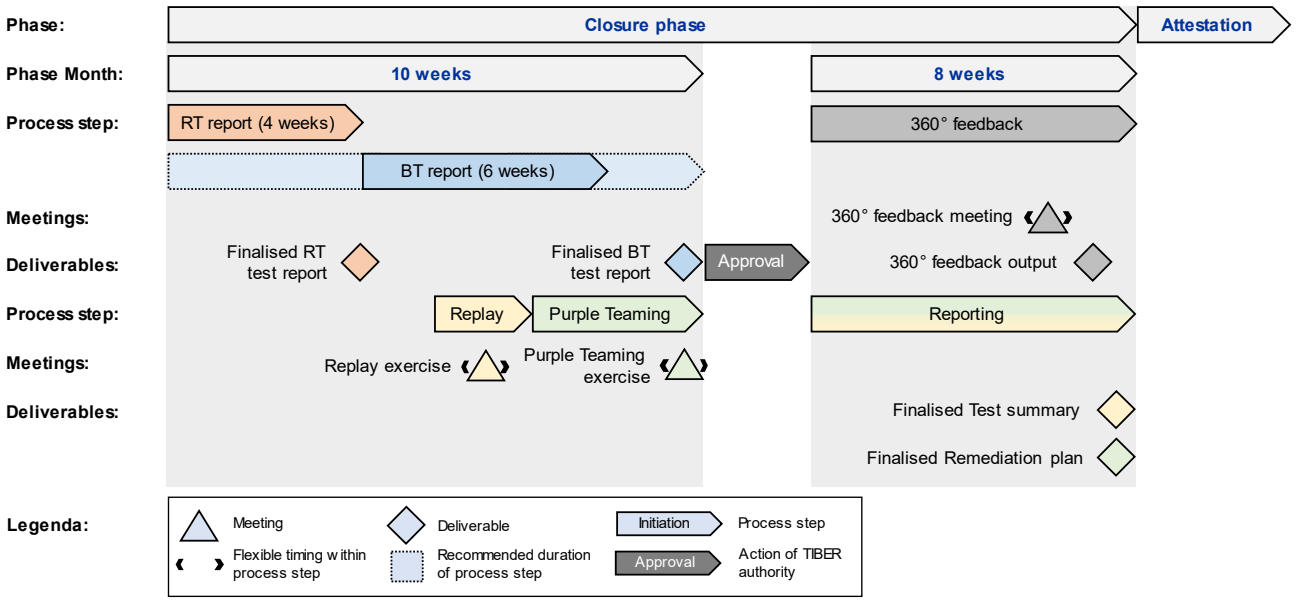
9 Closure phase

9.1 Overview

The closure phase allows all relevant stakeholders to reflect on the outcome of the test and make improvements to further enhance the cyber resilience of the entity. Once the active testing is concluded and the BT has been informed about the test, the RTT and the BT start to create their respective test reports. The RTTP includes details of the approach taken to the testing and the findings and observations from the test, whereas the BT Test Report (BTTR) includes details on the observations of the BT during the test, mapped alongside the actions of the RTT.

Once these reports are in a final stage, the replay process step commences, followed by the PT process step. After the replay and PT process steps, the CT finalises the test summary report and remediation plan. When the PT step has concluded, the 360°-feedback process step commences, during which all relevant stakeholders deliver feedback on each other, and the overall testing process. The test is concluded with remediation planning and result sharing. A process overview of the closure phase can be found in the figure below[28].

Figure 6
Closure phase process overview



[28] The figure only includes the actions of the TIBER authority that have an impact on the timelines of the test. The figure is not an exhaustive overview of all actions to be undertaken by the involved stakeholders.

The first part of the closure phase, containing the writing of the RTTR and BTTR and the replay and PT exercises, takes a maximum of 10 weeks. The second part of the closure phase relates to the TM's assessment of the BTTR and the RTTR. The third part of the closure phase, related to the 360° feedback and the writing of the test summary report and the remediation plan, takes a maximum of 8 weeks. Finally, the closure phase ends with the test attestation. Depending on the time the TM needs for the assessment of the RTTR and BTTR, the total duration of the phase may be longer than 18 weeks.

9.2 Red Team Test Report and Blue Team Test Report creation

These process steps commence after the active testing has been concluded and the key members of the entity's BT are informed about the test. The RTT produces a RTTR, for delivery to the CT within four weeks from the end of the active red team testing phase, which in turn delivers it to the BT and the TM. It is then used by the BT to deliver the BTTR, no later than 10 weeks after the end of the active red team testing phase, to the CT, which in turn delivers the BTTR to the RTT and TM. The BTTR should be drafted ahead of the replay and PT exercises. In the BTTR, the BT maps its actions alongside the RTT's actions. Both reports are expected to contain a timeline of events and detections that occurred during the exercise together with any other relevant information.

It is important to note that the RTTR and BTTR are highly sensitive. As such, access to these reports, their dissemination, retention and destruction must be controlled. At the request of the TM, the reports might be cleared of sensitive information[29].

The TM assesses that the RTTR and BTTR contain the required information and provides feedback where necessary. Given the importance of the RTTR for the BTTR and the replay exercise, the TM is advised to provide feedback on the document once in a final stage.

[29] Such as machine names, IP addresses, etc.

Deliverable: RTTR

The RTTR should include at least the following information:

1. Information on the performed attack, including:
    a. the targeted CIF and identified ICT systems, processes and technologies supporting the CIF, as identified in the RTTP.
    b. summary of each scenario;
    c. flags reached and not reached;
    d. attack paths followed successfully and unsuccessfully;
    e. TTPs used successfully and unsuccessfully;
    f. deviations from the RTTP; if any;
    g. leg-ups granted, if any.

2. All actions that the RTT are aware of that were performed by the BT to reconstruct the attack and mitigate its effects.

3. Discovered vulnerabilities and other findings, including;

    a. a description of the vulnerabilities and other findings, as well as their criticality;
    b. a root cause analysis of successful attacks;
    c. recommendations for remediation and an indication of the remediation priority.

The RT should deliver the RTTR to the CT, which in turn delivers it to the BT and TM, within four weeks after the end of the active testing phase.

Available guidance: TIBER-EU Red Team Test Report Guidance

Deliverable: BTTR

The BTTR should at least include the following elements and information:

1. For each attack step described by the testers in the RTTP:
    a. a list of detected attack actions;
    b. log entries corresponding to these detections.

2. An assessment of the findings and recommendations of the testers.
3. Evidence of the attack by the RTT collected by the BT.
4. BT root cause analysis of successful attacks by the testers.
5. List of lessons learned and identified potential for improvement.
6. List of topics to be addressed in the PT exercise.

The BT should deliver the BTTR within 10 weeks after the end of the active testing phase to the CT, which in turn delivers it to the RTT and TM.

Available guidance: TIBER-EU Blue Team Test Report Guidance

9.3 Replay exercise

After the RTT and BT deliver their reports, the CT arranges a replay exercise. Although the exercise should be held within 10 weeks after the end of the active red team testing, it is highly recommended for the exercise to take place after the BTTR

has reached a substantial form. The goal of this exercise is to learn from the testing experience in collaboration with the RTT.

During the replay exercise, the RTT and BT jointly go through the actions each of the teams has taken during the test, based on the timeline of events agreed to in the reports. They discuss the conducted attack steps and all related issues of interest to allow the BT to gain a deeper understanding of the technical workings behind the actions taken by the RTT and the established or potential future countermeasures.

The findings and learnings of the replay exercise will feed directly into the final Test Summary Report (TSR) and remediation plan.

Meeting: replay exercise

During the replay exercise, the RTT and the BT go through the tested scenarios step by step to discuss:

- the progression through attack stages of each scenario and relevant learning generated;
- what else could have been achieved by the RTT with more time and resources;
- potential remediation measures;
- general questions from the BT.

The replay exercise must take place within ten weeks after the end of the active testing.

Participants to this exercise are, at least: the CT, BT, RTT, TM (if feasible).

9.4 Purple Teaming exercise

After the completion of the replay exercise, a PT exercise should be conducted, in which the RTT and the BT come together to discuss all remaining or additional topics relevant to the CT and the BT. This exercise is highly beneficial for increasing the learning experience of the entity, anchoring the learnings of the test within the organisation. Potential topics for the PT exercise should be jointly identified by the CT, RTT and the BT and could range from a table-top discussion to technical walkthroughs of the systems.

During the PT exercise, the BT and the RTT further elaborate on the scenarios that have been played out. This exercise allows the stakeholders to discover alternative scenarios and their potential consequences, maximising the learning effect of the overall test.

Although the exercise should be held no later than 10 weeks after the end of the active red team testing, it is highly recommended for the exercise to take place after the BTTR has reached a substantial form.

Meeting: PT exercise

During the PT exercise, the RTT and the BT discuss all remaining or additional topics relevant to the CT and the BT, such as:

- relevant issues that could not be tested during the active testing phase particular vulnerabilities identified during the test;
- other steps which could have been taken by the RTT and potential BT responses;
- alternative scenarios and their potential consequences;
- proof of concepts;
- discussion of anticipated remediation measures with the RTT;
- business continuity exercises.

The PT exercise must take place within ten weeks after the end of the active testing.

Participants to this exercise are at least: the CT, BT, RTT.

Available guidance: TIBER-EU Purple Teaming Guidance

9.5 Test Summary Report

The TSR highlights the overall test process and results, and should draw on the test documentation, such as the RTTR, the BTTR, the TTIR as well as the RTTP.

The entity should be aware of the sensitivity of the TSR. Sensitive, detailed technical information about findings and identified vulnerabilities at a detailed level, may cause great risks in the wrong hands.

The TSR should be delivered by the entity to the TM[30], within eight weeks after the TM has sent a notification of the completed assessment of the RTTR and BTTR[31]. The TM shall approve the TSR. If requested by the TM, a version not containing any sensitive information[32] should be provided instead.

[30] When conducting a TIBER test to fulfil testing requirements under the DORA regulation, it needs to be made sure that the report is also sent to the respective competent authority, if not already acting as a TIBER authority.

[31] It is highly recommended to obtain feedback from the TM before sending the final version for approval by the TIBER authority.

[32] Such as machine names, IP addresses, etc.

Deliverable: Test Summary Report

The findings and learnings of the replay and PT exercises will feed directly into the final TSR. The TSR must include at least:

1. the parties involved;
2. the project plan;
3. the validated scope, including the rationale behind the inclusion or exclusion of CIFs and identified ICT systems, processes and technologies supporting the CIFs covered by the test;
4. selected scenarios and any significant deviation from the TTIR;
5. executed attack paths, and used TTPs;
6. captured and non-captured flags;
7. deviations from the RTTP, if any;
8. BT detections, if any;
9. PT in testing phase, where conducted and the related conditions;
10. leg-ups used, if any;
11. risk management measures taken;
12. identified vulnerabilities and other findings, including their criticality;
13. root cause analysis of successful attacks;
14. high level plan for remediation, linking the vulnerabilities and other findings, their root causes and remediation priority;
15. lessons derived from feedback received.

The TSR must be delivered to the TM for approval within eight weeks after the assessment notification of the RTTR and BTTR by the TM.

Available guidance: TIBER-EU Test Summary Report Guidance.

9.6 Remediation plan

The remediation plan is, in addition to the replay and PT exercises, also based on the TTIR, BTTR and RTTR. Its aim is to plan improvements and the mitigation of vulnerabilities (and their root causes) identified during the test.

The remediation plan should be delivered to the TM[33], within eight weeks after the TM has sent a notification of the completed assessment of the RTTR and BTTR[34]. If requested by the TM, a version not containing any sensitive information[35] should be provided instead.

[33] When conducting a TIBER test to fulfil testing requirements under the DORA regulation, it needs to be made sure that the report is also sent to the respective CA, if not already acting as a TIBER authority.

[34] It is highly recommended to obtain feedback from the TM before sending the final version for approval by the TIBER authority.

[35] Such as machine names, IP addresses, etc.

Deliverables: Remediation plan

The findings and learnings of the replay and PT exercise will feed directly into the remediation plan.

The elements to be covered in the remediation plan are:

(a) a description of the identified shortcomings;

(b) a description of the proposed remediation measures and of their prioritisation and expected completion, including where relevant measure to improve the identification, protection, detection and response capabilities;

(c) a root cause analysis;

(d) the entity's staff or functions responsible for the implementation of the proposed remediation measures or improvements;

(e) the risks associated to not implementing the measures referred to in point (b) and, where relevant, risks associated to the implementation of such measures.

The remediation plan should be delivered to the TM, within eight weeks after the TM has sent a notification of the completed assessment of the RTTR and BTTR.

Available guidance: **TIBER-EU Remediation Plan Guidance**

9.7 360° feedback

After the completion of the replay and PT exercises, the 360° feedback process step takes place. The TM participates in the 360° feedback process step but is not obliged to provide feedback. The dedicated 360° feedback meeting, organised by the TM, is focussed on providing feedback to all the stakeholders involved in the testing process. This meeting allows for the participants in the test to reflect upon and improve their approach for future tests. In addition, it also creates the possibility to provide feedback on the testing process as well as the TIBER-EU framework.

Meeting: 360° feedback meeting

During the 360° feedback meeting, the stakeholders come together to review the conduct of the test. All parties should deliver feedback on each other and on the overall process to facilitate the learning experience for future exercises. TM feedback is optional. The key topics to be covered in the 360° feedback output, from all parties' perspectives, are:

- which activities/deliverables could have been improved;
- which aspects of the TIBER process worked well;
- which aspects of the TIBER process could be improved;
- any other feedback.

Participants to this meeting are, at least: the CT, TIP, RTT, BT and the TM.

The 360° feedback meeting should take place before the TM approval of the TSR and the remediation plan.

Deliverable: 360° feedback output

During the 360° feedback process step, the stakeholders should each finalise and share their respective written 360° feedback. Although not obliged, the TM may provide feedback as well.

All stakeholders should deliver and receive their written feedback before the TM approval of the test summary and the remediation plan.

The TM may share the output from the 360° feedback on an anonymous basis with the TKC so that all lessons learned can be reflected on and improvements can be made to the TIBER-EU framework. This is a key part of the "learning and evolving" principle that underlies the TIBER-EU framework.

9.8 Attestation, result dissemination and follow-up

At the end of the test, once the TIBER authority has approved the TSR as well as the remediation plan, the TIBER authority should provide an attestation confirming that the test was conducted in accordance with the core requirements of the TIBER-EU framework. The attestation should be signed by the TIBER authority[36]. The issuing of the attestation concludes the TIBER test.

[36] Please note that for the conduct of a TIBER test to fulfil testing requirements under the DORA regulation, the respective TLPT authorities are also regarded as TIBER authorities.

Deliverable: Attestation

The attestation should include at least the following information:

a. the starting and end dates of the test;

b. the CIFs in scope of the test;

c. CIFs in scope of the test that were not tested;

d. where relevant, other entities that were involved in the test;

e. where relevant, ICT third-party service providers that participated in the test;

f. whether internal testers were used;

g. whether or not the TIP and RTT met the required standards as defined in the Guidance for Service Provider Procurement;

h. the duration of the active RT testing phase, expressed in calendar days;

i. when applicable, the other TIBER authorities that have been involved in the test, and in which capacity;

j. a list of the documents examined by the TIBER authority for the purpose of the attestation.

Available guidance: TIBER-EU Attestation Guidance

A TIBER test attestation can serve as a means of qualifying the test for mutual recognition among other authorities. In cases where other TCTs did not participate in the test but there was mutual agreement to share the test results, the entity should share the TSR, the remediation plan and the attestation. The TSR serves as a form of assurance that the test has indeed been conducted, and the attestation qualifies the test as a legitimate TIBER test.

As one of the key objectives of the TIBER-EU framework is to enhance sector resilience, the TCT of each jurisdiction should analyse the results of all the tests to identify the key findings, common threats and vulnerabilities, and to disseminate these in the appropriate form to relevant stakeholders. The TCT may also share anonymised findings or lessons learned from their respective TIBER tests with the TKC. This information will allow the TKC to aggregate the key findings, common threats and vulnerabilities, to form a picture of the resilience of the European financial sector, and to bring about improvements where feasible. In all cases, any exchange of information should be conducted in a safe and secure manner.

From the outset, and without prejudice to existing regulations, it is up to the authority adopting the TIBER-EU framework to determine the role of the overseer and supervisor in the TIBER-XX implementation. In some cases, the authority may opt to include the overseer and supervisor throughout the entire testing process, while in some jurisdictions the authority may opt to formally exclude the involvement of the overseer and supervisor.

The respective competent authority might follow up on the results of the TIBER engagement, including the remediation plan. However, it is important to note that TIBER is a learning experience for self-improvement and that TIBER tests are snapshots rather than comprehensive assessments. The follow-up of results should therefore be conducted in the appropriate spirit.

10 Annex

10.1 Responsibility Assignment Matrix for a TIBER-EU test

Table 5
RACI Matrix, clarifying the roles and responsibilities within a TIBER-EU test.

Requirement	Responsible	Accountable	Consulted	Informed	Relevant documents
Preparation phase					
Notification letter	TIBER authority	TIBER authority	TCT	Management body of the entity	n/a
Assignment of TM	TCT	TCT	n/a	TM, Management body of the entity, TIBER authority	n/a
Appointment of CTL	Management body of the entity	Management body of the entity	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	Management body of the entity	TM	n/a	TIBER-EU Control Team Guidance
Initiation meeting	CTL	Management body of the entity	TM	n/a	n/a
Validation Initiation documents	TM	TCT	n/a	CTL	n/a
Validation CT composition	TM	TCT	n/a	CT	n/a
Procurement process and formal contracts between the different stakeholders	CTL	Management body of the entity	TM (non-objection)	TIP/RTT	TIBER-EU Guidance for Service Provider Procurement
Launch meeting	CTL	Management body of the entity	TM, TIP/RTT	n/a	n/a
Scope specification document	CTL	Management body of the entity	TIBER authority, TM	TIP/RTT, once available	TIBER-EU Scope Specification Document
Scoping meeting	CTL	Management body of the entity	TM	TIP/RTT, if available	n/a
Validation Scope specification document	TM	TCT	TIBER authority	Management body of the entity	n/a
Risk assessment	CTL	Management body of the entity	TM (non-objection)	TIP/RTT	n/a
Testing phase: threat intelligence					
Scenario selection meeting	CTL, TIP	CT	TM, RTT	n/a	n/a
Scenarios created	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 Targeted Threat Intelligence Report	TM, CTL	TM, CT	n/a	TIP	n/a
Testing phase: red team testing					
Red Team Test Plan	RTT	CTL	CT, TM, TIP	n/a	TIBER–EU Red Team Test Plan Guidance
Red Team Test Plan meeting	CTL, RTT	Management body of the entity	CT, TM, TIP	n/a	n/a

Requirement	Responsible	Accountable	Consulted	Informed	Relevant documents
Approval Red Team Test Plan	TM, CT	TM, CT	n/a	RT testers	n/a
Weekly test meetings or updates	CTL, RTT	CTL	TM, TIP, if requested	n/a	n/a
Provision Leg-ups, if necessary	CT	Management body of the entity	RTT, TM	n/a	n/a
Closure phase					
Blue Team briefing	CTL	Management body of the entity	n/a	BT	n/a
Red Team Test Report	RTT	CTL	n/a	BT, TM	TIBER-EU Red Team Test Report Guidance
Blue Team Test Report	BT	CTL	RTT	CT, RTT, TM	TIBER-EU Blue Team Test Report Guidance
Assessment 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
Test Summary Report	CT	Management body of the entity	TIP/RT testers	TM	TIBER–EU Test Summary Report Guidance
Approval Test Summary Report	TM	TM	n/a	CT, TIBER authority	n/a
Remediation Plan	CT	Management body of the entity	n/a	TM, TIBER authority	n/a
Expert opinion on eligibility for attestation	TM	TM	CT, TIP, RT testers	TIBER authority	n/a
Attestation	TIBER authority	TIBER authority	TM	n/a	TIBER-EU Attestation Guidance

10.2 Mandatory requirements of TIBER-EU process

Table 1
Adoption and implementation

Requirements	Mandatory	Optional
If a jurisdiction decides to implement a TIBER-XX framework, then the framework is formally adopted by one or multiple authorities, and the TIBER-EU Knowledge Centre is informed.	✓	
The jurisdiction adopts the TIBER-EU framework as a supervisory / oversight tool, as a catalyst, for the purposes of financial stability, or to fulfil regulatory requirements.	✓	
The jurisdiction publicly announces the implementation of the TIBER-XX framework.	✓	
The national or European TIBER-XX implementation document (and any updates to it) together with any accompanying documentation is submitted to the TKC for review and comments prior to publication.	✓	
On adoption, the national TIBER-XX implementation document is published, and the sector is informed. The implementation document contains at least: a) the official statement of adoption, b) the contact details of the TCT, c) national particularities of the implementation, d) reference to TIBER-EU framework and guidance.	✓	
The implementation document contains or refers to additional operational guidance.		✓
The jurisdiction determines which entities should undertake a test – either on a voluntary or mandatory basis.	✓	
The jurisdiction conducts a legal analysis of its TIBER-XX implementation document to ensure it complies with national laws and regulations.	✓	
The jurisdiction puts in place appropriate governance structures and allocates adequate resources to implement the TIBER-XX programme.	✓	
The jurisdiction has a TIBER Cyber Team (TCT) to manage the programme, oversee the tests and liaise with the TIBER-EU Knowledge Centre.	✓	
In case of cross-border entities, the test is initiated and driven by the lead authority. The lead authority is established after consultation with other authorities involved.	✓	
The TIBER-EU test is conducted by independent third-party providers, i.e. external Threat Intelligence Providers (TIP) and Red Team Testers (RTT). In exceptional cases internal RTT may be used after TM approval.	✓	

Table 2
Preparation phase

Requirements	Mandatory	Optional
For each test, there is a Control Team (CT) led by a Control Team Lead (CTL) from the entity undergoing the test, a Test Manager and an alternate from the TCT of the TIBER authority responsible for TIBER in the relevant jurisdiction, and an external TIP and dedicated RTT.	✓	
Once the procurement process has been completed, there are appropriate contracts in place between the different stakeholders, with relevant controls embedded into the contracts, to facilitate a controlled test (in a discreet manner).	✓	
Prior to conducting the test, the CT conducts a risk assessment and then puts in place all the necessary risk management controls, processes and procedures to facilitate a controlled test. These are documented in the entity's dedicated Risk Management Document.	✓	
Throughout the end-to-end test process, in all documentation and communication between stakeholders a code name is used to conceal the identity of the entity being tested, where appropriate.	✓	
During the preparation phase, there is a notification, initiation & launch meeting which includes the CT and TCT.	✓	
The launch meeting also includes the TIP/RTT. If applicable, the launch meeting may also include other relevant authorities.		✓
The scope of the test includes all critical or important functions (CIFs), as well as the people, processes, and technology that support the delivery of CIFs. This is documented in the TIBER-EU Scope Specification document and signed off by the management body of the entity.	✓	
The entity expands the scope of the test beyond the CIFs and includes other important functions, processes and third parties		✓
During the scoping phase, the CT (with agreement from the TM), sets "flags", refined by the TIP, which are targets or objectives, that the RTT aim to meet during the test.	✓	
The test may utilise the entire ICT infrastructure as a way to reach the "flags" and is conducted on live production systems.	✓	
Only the CT is informed about the test, its details and the timings – all other staff members (i.e. Blue Team, BT) remain unaware of the test.	✓	
Only TIP/RTT that are free from conflict of interest and meet the minimum requirements set out in the TIBER-EU Guidance for Service Provider Procurement can undertake the TIBER-EU test.	✓	

Table 3
Threat intelligence and red team testing phase

Requirements	Mandatory	Optional
For each test, an external TIP produces a dedicated Targeted Threat Intelligence report (TTI report) on the entity being tested. Where infrastructure has been outsourced and a third party is included in the scope of the test, the TTI report also includes information about that third party.	✓	
For each national implementation, a Generic Threat Landscape Report (GTL Report) for the country's financial sector is produced and maintained, and is used to help inform the TTI report.		✓
For each threat intelligence report (TTI and GTL), the national intelligence agency/national cyber security centre/high-tech crime unit is involved to provide feedback.		✓
For each TTI report on the entity, the TIP sets out multiple threat scenarios which can be used by the RTT.	✓	
The TIP continues to be engaged during the testing phase and provides additional up-to-date, credible threat intelligence to the RTT, where needed.	✓	
Based on the TTI report, the RTT refine the attack scenarios. This is documented in the Red Team test plan and shared with the CCT and TM.	✓	
The jurisdiction, in its implementation of the TIBER framework, allows physical red teaming in the scope of the methodology for the TIBER test (e.g. planting a device at the entity), provided all necessary precautions are taken.		✓
The RTT execute the attack based on the scenarios (with some flexibility) in the Red Team test plan and goes through each of the phases of the kill chain methodology. Where needed, a "leg-up" will be provided by the CT.	✓	
During the test, the RTT keep the CT and TM informed about progress, "capture the flag" moments, the possible need for leg-ups, etc. The RTT take a stage-by-stage approach and consults the CT and TM at all critical points to ensure a controlled test.	✓	
The duration of the red team test is proportionate to the scope, size of the entity, complexity of threat scenarios, etc. Sufficient time is allocated to testing to guarantee that a comprehensive test has been conducted across the enterprise, with a minimum duration of 12 weeks active testing.	✓	

Table 4
Closure phase

Requirements	Mandatory	Optional
At the end of the test, the RTT produce a Red Team Test Report (RTTR), outlining the findings from the test.	✓	
The entity's BT is informed of the test and uses the RTTR to deliver its own Blue Team report. In the Blue Team report, the BT maps its actions alongside the RTT actions.	✓	
At the end of the test, the RTT, the BT and the CT conduct an interactive replay of the test, where possible using live production systems, to review the impact of the actions of the RT provider.	✓	
The TM, supervisors/overseers and TIP are also present during the replay exercise.		✓
During the purple teaming exercise, the BT and the RTT work together to see which other steps could have been taken by the RTT and how the BT could have responded to those steps.	✓	
At the end of the test, there is a 360-degree feedback meeting which includes the entity, TIP/RTT and TM. In this meeting, the parties review the TIBER-EU test process and give feedback.	✓	
After the replay & Purple Teaming exercises, and the 360-degree feedback process step, the entity produces a remediation plan to address the findings (from both TTIR, RTTR).	✓	
The entity produces a Test Summary report, which it shares with the TIBER authority.	✓	
The TIBER authority provides the entity with an attestation to validate the true and fair conduct of the TIBER-EU test (to enable recognition by other relevant authorities).	✓	
If mutually agreed or legally mandated, the TIBER authority and/or the entity share the Test Summary report, Remediation Plan and Attestation with other relevant authorities (where applicable).	✓	

Abbreviations

Term	Explanation
BT	Blue Team
BTTR	Blue Team Test Report
CIF	Critical or Important Function
CSP	Critical Service Provider
CT	Control Team
CTL	Control Team Lead
CTI	Cyber Threat Intelligence
DORA	Digital Operational Resilience Act
ESCB	European System of Central Banks
GTL	Generic Threat Landscape
HUMINT	Human Intelligence
ICT	Information and Communication Technology
ISAC	Information Sharing and Analysis Centre
NDA	Non-Disclosure Agreement
OSINT	Open-Source Intelligence
PT	Purple Teaming
RACI	Responsibility Assignment Matrix (RACI stands for Responsible, Accountable, Consulted, Informed)
RTT	Red Team Testers
RTTP	Red Team Test Plan
RTTR	Red Team Test Report
TCT	TIBER Cyber Team
TIBER	Threat Intelligence-Based Ethical Red Teaming
TIP	Threat Intelligence Provider
TKC	TIBER-EU Knowledge Centre
TLPT	Threat Led Penetration Testing
TSR	Test Summary Report
TI	Threat Intelligence
TTIR	Targeted Threat Intelligence Report
TM	Test Manager
TTP	Tactics, Techniques and Procedures

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

For terminology and abbreviations, please refer to the ECB glossary.