TIBER-PT
GENERAL IMPLEMENTATION GUIDE

TIBER-PT
GENERAL IMPLEMENTATION GUIDE

MAR. 2022

BANCO DE PORTUGAL
EUROSISTEMA

Lisboa, 2022 • www.bportugal.pt

Table of Contents

Change Log

Version	Date	Comments

1 Introduction

1.1 Background

In a context of increasing digitalization in the banking sector, ensuring an adequate degree of operational and particularly cyber resilience maturity is of great importance, both to control entities' individual risk levels as well as risks for the stability of the financial system. Furthermore, there is a perception of an increase in cyber threats associated with large scale events (e.g. ransomware attacks on a number of businesses across the world, including in the EU). The data in Portugal show that the reality of increasing intensity of cyber-threats is no different than in other jurisdictions[1].

In this sense, threat-intelligence led penetration testing of critical production systems, while sensitive, is key to help an entity to better assess its protection, detection and response capabilities, as opposed to penetration tests, which while also an important tool to assess the efficiency of the existing cyber security controls and detect technical and configuration vulnerabilities, are usually limited in scope, as they do not assess the full scenario of a targeted attack against an entire entity (people, processes and technologies), focusing mostly on the IT systems and respective logical preventive measures.

Threat intelligence based ethical red teaming (TIBER) simulates the tactics, techniques and procedures (TTPs) of advanced threat actors who pose a significant threat to entities, against live critical production infrastructure, in a way that realistically tests an entity's defences and provides a unique learning opportunity to the entity.

The purpose of the implementation of the TIBER-EU framework in Portugal (TIBER-PT) is to follow the sector's best practices as established by the TIBER-EU framework, the EBA Guidelines on ICT and security risk management (paragraph 43b of EBA/GL/2019/04)[2].

During the implementation of TIBER-PT, it is expected to use governmental and commercial threat intelligence, adjusted to what are the entities' business models and operations. In order to enable ethical red team testers to accurately simulate real-life attacks from malicious entities tests are executed on live production systems.

TIBER-PT tests shall be performed only with a very limited number of persons within the entity to be tested (target entity) being aware of the test, who are referred to as the White Team (WT), and avoiding that the target entity's cybersecurity and incident response capabilities (Blue Team [BT])

[1] CNCS - Observatório de Cibersegurança

[2] Guidelines on ICT and security risk management | European Banking Authority (europa.eu)

acknowledge or prepare for the threat beforehand. This allows for a better assessment of how effectively the entity is able to protect its systems that underpin its critical functions (CF), and how effectively it can detect and respond to attacks. It is critical that all relevant stakeholders keep each other informed at all stages to ensure the success of the test.

Due to the critical nature of the live production systems subject to a TIBER-PT test, the framework sets out a number of risk management activities to ensure a controlled test.

1.2 Purpose of this guide

The purpose of TIBER-PT is to foster a collaborative environment and the enhancement of the cyber resilience and consequently the stability of the financial system in Portugal, in line with the Statute of Banco de Portugal[3].

This guide has been developed by the TIBER Cyber Team (TCT) of the TIBER-PT authority, i.e. Banco de Portugal (BdP), in close cooperation with a technical working group comprised of other relevant authorities, as well as some of the largest credit institutions operating in Portugal, on a voluntary basis. It is meant to benefit the entities that aim to undergo TIBER-PT participants tests and their stakeholders as well as the external TI and RT providers, by providing guidance on the key phases, activities, deliverables and interactions involved in a TIBER-PT test.

The aim of this document is not to provide strict rules for the TIBER-PT tests but rather to provide general guidelines on how to conduct it. It should therefore be read alongside other relevant TIBER-PT and TIBER-EU framework and supplementary guidance, which will be provided by the TCT to TIBER-PT participants, as well as the relevant regulation and legislation. The TCT is available to answer any questions that involved entities might have regarding TIBER-PT.

1.2.1 Review clause

Banco de Portugal will periodically review and update this Guide at least every three years and whenever there are relevant changes to the context of the Guide namely material changes to the TIBER-EU framework or material changes in the EU legal framework for the provision of financial services.

[3] See articles 12 (c) and (d) of the Statute of Banco de Portugal, approved by Law No 5/98 of 31 January 1998 and subsequently amended.

2 TIBER-PT overview

2.1 Target group

TIBER-PT's main objective is to strengthen the cyber resilience of financial entities and to mitigate possible systemic effects. Therefore, the target group of entities to be tested are broadly defined as including credit institutions, financial holding companies and mixed financial holding companies (Article 93 of Decree-Law No 298/92), payment institutions and electronic money institutions (Article 117-A of Decree-Law No 298/92) under the supervision of BdP and other financial entities subject to either the direct supervision or oversight of BdP[4]. The intent of this broad definition is to allow for the inclusion of voluntary one-off assessments, as well as the evaluation by the TCT of possible entities to be considered for a TIBER-PT test, in accordance with their criticality and cyber resilience maturity. In which case, the TCT may approach those entities to jointly discuss the possibility of conducting a TIBER-PT test. In this sense, the target group may be reviewed in later versions of this guide to specify other types of entities included in scope.

For a TIBER test to be fruitful, it is essential that the target entities possess a certain level of cyber resilience maturity. This means that while the entity might possess major gaps in its cybersecurity controls, which may not necessarily block the execution of a TIBER test, it may limit the benefits of doing such a test, as only after overcoming these issues may there be a greater focus on entity-specific vulnerabilities.

In the case of entities from other countries that operate in Portugal through a subsidiary or branch, these can also partake in a TIBER-PT test, dependant on their significance to the CFs and after consultation of their home country TIBER-XX authority. In these instances, the TIBER tests shall be conducted as a joint venture with the TCTs from all authorities involved (i.e., the TIBER-PT authority; the TIBER-XX authority from the target entity home country; other TIBER-XX authorities dependant on the geography of the target entity's CFs; and the European Central Bank, which may also be involved in case of pan European entities) to avoid duplication of work. The authorities involved in a multi-jurisdictional TIBER test, as well as the lead TIBER authority (i.e., the authority leading the TIBER-PT test), are decided on a case-by case basis, taking into consideration the coverage and location of the entity's critical economic functions, and agreed between authorities.

2.2 Main stakeholders and responsibilities in TIBER-PT

A TIBER-PT test requires the involvement of a number of different stakeholders with clearly defined roles and responsibilities in the TIBER-PT test, namely the TCT, WT, Red Team (RT) provider and Threat Intelligence provider (TIP). All main stakeholders involved in a TIBER-PT test should be well informed about their respective roles and responsibilities to ensure that the test is conducted in an adequate and controlled manner. There is a workflow in place that ensures that all relevant

[4] For the current version of this guide, the approach of the TCT is to consider only credit institutions for the purpose of TIBER-PT tests. However, other entities can be included in future versions.

stakeholders are informed (on a need to know basis) of the status of the project and that there is a protocol in place for information sharing and storage during and after the tests are concluded. Moreover, the BT will be involved in the test, as it will be responsible for detecting and responding to the controlled attacks of the TIBER-PT test, which is unbeknownst to them, until the closing phase where they will be actively and knowingly involved to maximise the value learning experience.

The TCT is the national competence centre for TIBER-PT implementation, and is located within the BdP. It provides support and specialist knowledge during the TIBER tests throughout all phases, ensures compliance with TIBER test requirements, certifies TIBER tests 'alignment with the framework once they have been completed and acts as the contact point for all external enquiries. The TCT can remove the TIBER label from a test if it has not been carried out in accordance with the requirements and spirit of the TIBER-EU framework and TIBER-PT Guide. The TCT may also, as a last resort, escalate any major deviations from the TIBER methodology to its direct report line in BdP or/and the target entity's executive members (e.g. CEO, COO or CISO).

To ensure an efficient support to the tests, the TCT may consult with national security authorities (e.g. the National Centre for Cybersecurity) if necessary, always with a commitment to the secrecy required in such case.

The WT[5] is a team from the target entity whose members are aware of the test from the start. This team shall be composed of a restricted number of senior executives and management people, who are knowledgeable of the entity's CFs to be tested and have sufficient technical knowledge in their midst to understand and dispute scenarios, plans and conclusions provided by the RT.

The RT provider is the external service provider, procured by the target entity, to attempt to breach the security capabilities in place using ethical hacking methods. The RT plans and executes the TIBER test on the target entity's systems and services, as agreed in the scope.

The TIP uses multiple sources of intelligence to provide accurate and up to date threat intelligence scenarios applicable to the target entity. The TIP elaborates a Targeted Threat Intelligence (TTI) Report setting out the threat scenarios that can be used by the RT to develop attack scenarios.

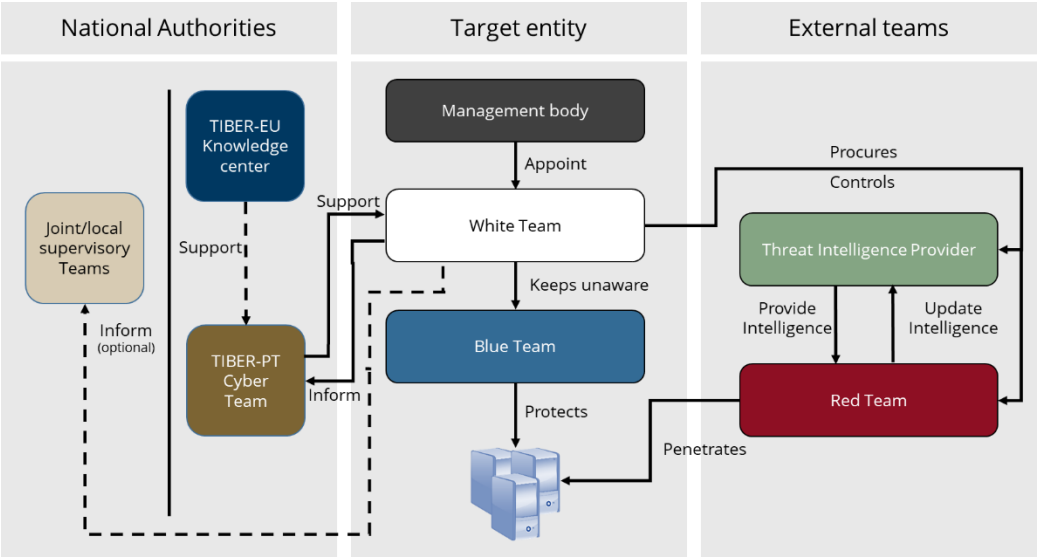
The TCT must have direct access to the TIP and RT provider when needed, for the whole duration of the TIBER-PT test.

In every TIBER-PT test, there will also be a BT which is defined as all staff at the target entity who are not part of the WT, which include but are not limited to the employees of the units responsible for cybersecurity. The BT shall only be informed of the tests in the closing phase, after the test execution has been completed. This is an essential element of the TIBER-EU framework, and therefore, the WT must implement controls to avoid that the BT detects that the scheduled attacks

[5] Further details on the WT's tasks and responsibilities are provided in the TIBER-EU White Team Guidance.

are part of a TIBER-PT test, and also avoid that they unknowingly inform the authorities of said attacks. Only during the closure phase shall the BT be informed of the test. At this stage, the relevant members of the BT should participate in the replay and follow-up of the test. The entities may at their discretion inform their joint and/or local supervisory teams of the results of the TIBER-PT test.

Figure 2.1 • Overview of the stakeholders involved in TIBER-PT.



2.2.1 Test management responsibilities

While an entity shall always conduct a TIBER-PT test in conjunction with the TIBER-PT authority (and other TIBER-XX authorities, in case of a cross-border test), the entity is entirely responsible for the TIBER-PT test from end to end. The responsibility for the overall planning and management of the test belongs to the WT, always with the involvement and agreement of the TCT.

The two main stakeholders in the management of a TIBER-PT test are the WT as the responsible on the side of the target entity and the TCT representing the respective TIBER-PT authority (in case of cross border tests, there may be more than one TCT, representing all the TIBER-XX authorities involved). The WT should have extensive knowledge of the entity's business model, functions and services, and provide the necessary information to the TCT, when requested.

The entity shall nominate the elements of the WT and which element shall be the White Team Lead (WTL). The WTL coordinates all test activity including engagement with the TIP and RT and is responsible for the coordination with the TCT. The WTL determines the scope, scenarios and risk management controls for the test. The WTL is also responsible for the coordination of the test activity including engagement with the TIP/RT and ensuring that the TIP/RTs project plans are factored into the entity's overall project planning for the TIBER-PT test. In case systems underpinning critical functions are either partially or totally outsourced, the target entity may include, after non objection from the TCT, a representative of the relevant third party provider in the WT (possibly with limited dedication and access only to information relating to that CF), to

ensure that this CF is adequately tested, with the same requirements as if the CF had not been outsourced.

Similarly, the lead TIBER authority will appoint a TCT for the specific test consisting of Test Managers and a Team Test Manager (TTM) from the TCT, who shall be responsible for overlooking the test, to ensure that the entity conducts the tests in a uniform and controlled manner, in line with the TIBER-PT test standards and with the test plan. If during the execution of a TIBER-PT test there are significant deviations from the original plan, the TTM must be involved in the discussion beforehand. The lead TIBER authority may also appoint one of the test managers as backup TTM either prior or during the execution of the TIBER test.

The TCT via the TTM may remove the TIBER label of a test at any point in the TIBER process if the requirements and spirit of the TIBER-EU framework and TIBER-PT implementation guide are not adhered to.

Both the WTL and TTM should have a formal escalation line, for critical decision making related to the scope or planning of the test, as well as for when differences of opinion persist. These formal lines shall consist of:

- for the WTL - the chief information security officer, the chief operating officer, the chief risk officer or any other appropriate senior personnel or Board member with sufficient decision-making authority in the target entity;
- for the TTM - the senior management, the board members, or any other appropriate senior personnel with sufficient decision-making authority from the lead TIBER authority and from other TIBER authorities involved, in case of a cross-border test).

The WTL must ensure that the entity's management body approves and attests the scope and risk management controls for the test. The TTM must also agree with the scope and the scenarios.

The primary contact for the TIP and RT provider is the WTL, but direct access must be provided to the TTM when required.

The TTM is not accountable for the WT's actions, the management of the test, the outcomes or the remediation planning. It is the responsibility of the WT to ensure that a fit and proper test is conducted in line with the requirements of TIBER-PT and that risks are managed throughout all phases.

The RT and TIP shall produce a planning for their services and inform the WT so that these plans can be incorporated in the overall TIBER-PT test project planning.

2.2.2 Test implementation responsibilities

The main stakeholders for the implementation of a TIBER-PT test are the TIP and RT. A TIBER-PT will only be recognized as such if both the TIP and RT provider are external to the target entity, to

ensure an independent and fresh outlook on the entity's cyber-resilience capabilities, as well as dedicated expertise on how to conduct TLPT.

The TIP is responsible for providing threat intelligence services using multiple sources of intelligence to provide an assessment that is as accurate and up to date as possible. The TIP must be willing to share its deliverables (once approved by the target entity) with the RT for review and comments, and work with the RT during the remainder of the TIBER-PT test, when needed, and in accordance with its function in the tests. The main deliverable from the TIP is the Targeted Threat Intelligence Report (TTI Report), which defines the threat scenarios to be accounted for by the RT in the development of the attack scenarios. The TIP is also expected to provide input into the Red Team Test report issued to the target entity.

The RT is responsible for planning and executing the TIBER-PT test on the entity's systems and services, in accordance with the agreed scope. The RT must be willing to work closely with the TIP. The RT is required to work with the TIP throughout the testing in order to update the threat intelligence assessment and attack scenarios with relevant threat intelligence data. Furthermore, the RT must review the TIP deliverables and develop the final report in conjunction with the TIP.

The RT should expand on and execute the established threat scenarios identified by the TIP and approved by the target entity, pending non objection by the TCT. The threat scenarios are developed from an attacker's point of view. As such, the RT should indicate various creative options in each of the attack phases based on the various TTPs used by advanced attackers. This is in order to anticipate changes in circumstances or in case some attack methods do not succeed during the test. The scenario development is a creative process, and thus, the TTPs employed in the test should not simply mimic scenarios seen in the past but should aim to combine the TTPs of various relevant threat actors. The RT should assess the cyber resilience posture of the target entity in light of the threat it faces.

The RT should follow a rigorous and ethical red teaming test methodology, and should meet the minimum requirements defined under the TIBER-PT framework. The rules of engagement and specific testing requirements should be established by the RT provider and the target entity. This is followed by a review of the test and issues arising, culminating in a Red Team Test Report drafted by the RT.

At all points during the implementation of a TIBER-PT test, the target entity shall remain in control of the process. Implementing and enforcing appropriate risk management controls for the execution of the TIBER-PT test is the responsibility of the target entity, and specifically the WTL. The TIP and RT shall at all times conduct the tests within the remit of all laws and regulations, and in accordance with the rules and limits determined by the WT. The TTM shall be closely involved in each test to ensure that the test proceeds according to the scope, scenario, planning and process agreed and described in the framework documents developed collaboratively.

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

During the process of the test, if the TCT suspects that the BT is aware of the test taking place, and has taken steps to manipulate the integrity of it, the TIBER-PT authority (together with the other TIBER-XX authorities in the case of a cross border test) may remove the TIBER label from the test and thus not recognise it as a TIBER-PT test. Knowledge of any issue compromising the test will be apparent through the continuous engagement between the TTM and RT.

2.3 Risk management

Due to the sensitive nature of a TIBER-PT test, that it is performed in the production environment, and the criticality of the systems involved, it is of the utmost importance to ensure that ensuing risks are managed efficiently throughout the test. The target entity, and specifically the WTL is the one responsible for ensuring that appropriate controls, processes and procedures are in place and that these are sufficient to mitigate the associated risks in accordance with the best practices in risk management. Thus, the target entity will be responsible for conducting a risk assessment prior to the test, and implement adequate risk management measures in line with its existing risk management framework.

Prior to any testing, the target entity must take the necessary measures to ensure that backup and restoration capabilities are in place for all in-scope systems.

The inclusion of physical testing methods (e.g. physical access to the network) is encouraged if in-line with the TTI, but is open to the WT to decide whether to include them in scope or not, as long as it does not conflict with current legislation or the entity's security requirements.

The entity shall use competent, qualified and skilled TI and RT providers with the requisite experience to conduct such tests. Prior to engagement, the entity must ensure that the TIP and RT provider meet the requirements set in the TIBER-EU Services Procurement Guidelines[6]. The target entity shall also do a thorough screening of the providers' technical capabilities, skills and resources to verify its adequacy to conduct a TIBER-PT test. Moreover, entities not yet or at the moment involved in a TIBER-PT test may assess when appropriate which TTI and RT providers might be sufficiently competent, qualified and skilled to conduct these tests, in preparation of future tests, to ensure the timeliness, agility and appropriateness of their choice of providers in the procurement phase in case they wish to start a TIBER-PT test.

The target entity and the respective TIP and RT provider must enter a mutual agreement, which must specify at least the following aspects: i) the scope of the test; ii) boundaries; iii) timing and availability of the providers; iv) actions to be taken; and v) liability (including insurance where applicable). Moreover, there must be a formal agreement on the following: security and confidentiality requirements to be met by the providers (at least as stringent as those followed by the target entity); provisions for the protection of those involved (e.g. indemnifications); a clause

[6] TIBER-EU Services Procurement Guidelines

related to data destruction requirements and breach notification provisions; a list of activities that are not allowed during the test, such as: destruction of equipment; uncontrolled modification of data/programs; jeopardising continuity of critical services; blackmail; threatening or bribing employees; and disclosure of results. Regarding personal data, it should only be collected and processed when absolutely necessary, and in accordance with applicable legislation.

The TIBER-EU Services Procurement Guidelines set out in greater detail agreement checklists for the entity and TIP/RT provider to consider and apply when formalising their contractual terms.

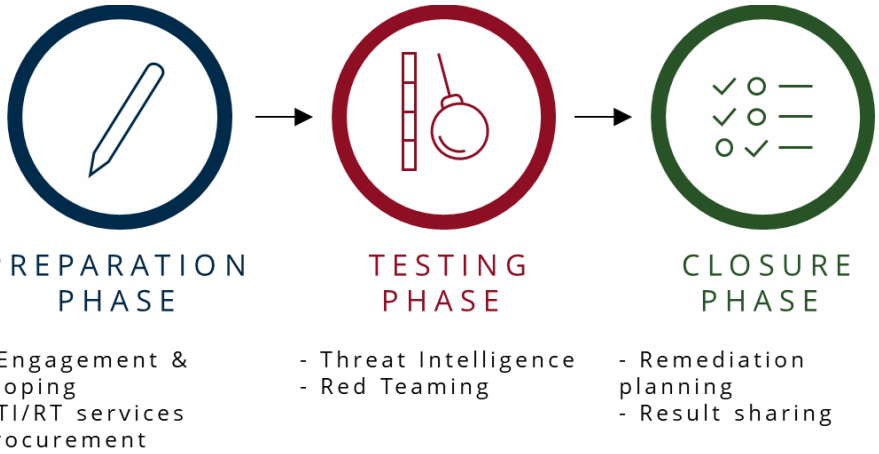
The target entity must implement measures to be taken to ensure that only the WT is informed about the test. The WT should also define escalation procedures to avoid the triggering of actions that would be mandatory in the case of a real cyber-incident, such as those related to reporting to external entities or bodies or criminal authorities. In this sense, all stakeholders must use code names for the target entities being tested, rather than explicitly naming the entities. All documentation and multilateral communication should refer to the target entity by the commonly agreed code name to protect its identity.

3 TIBER-PT testing process

Once BdP and the target entity agree to undertake a TIBER-PT test, the TIBER-PT TCT will inform the TCTs of all other relevant authorities, if needed, and the parties involved in the test should be briefed of the TIBER-PT process, documentation, roles and responsibilities.

A TIBER-PT test process consists of three mandatory phases: preparation, implementation and closure. These phases can overlap during a test (e.g. RT services procurement can occur while the TTI is developed, and remediation of issues can start while testing is still ongoing).

Figure 3.1 • Overview of the three phases of a TIBER test.



The TIBER-EU framework provides the option for the TIBER authorities to develop a generic threat landscape (GTL) report on the financial sector, which when available shall complement the TTI Report in the design of attack scenarios by the RT.

The GTL report is an assessment of the national financial sector threat landscape, outlining the specific roles of the entities, identifying the relevant high-end threat actors for the sector and the TTPs targeting these entities. For the time being, there is no GTL report in Portugal.

Once BdP develops the GTL report, it will be made available to entities at the start of each preparation phase of a TIBER-PT test, so that the information it contains can complement that of the TTI Report and serve as basis for the scenario development. BdP will also update this report periodically or whenever new threat intelligence information is obtained and deemed relevant for future TIBER-PT tests.

3.2 Preparation Phase

During the preparation phase the TIBER-PT authority (or the lead authority in the case of a cross border test) starts the engagement with the entities to be tested and the teams responsible for managing the test from both sides are established. Moreover, the scope of the test is determined, approved and attested by the target entity's board, and validated by the TIBER-PT authority (and other authorities, in case of a cross border test). The target entity starts the procurement of the TIP and RT provider to carry out the test.

This phase lasts approximately four to six weeks, not including the duration of the target entity's procurement process.

Figure 3.2 • Overview of the preparation phase.

The TTM asks the target entity to establish a WT, which shall comprise a selected number of individuals with sufficient technical and business know-how (e.g. cyber, operational and risk specialists, experts from the business areas that support the CFs, etc.) and that are positioned at the top of the security incident escalation chain (the composition shall be adjusted in accordance with the target entity's own organisational structure). The target entity nominates a WTL.

The WTL holds the **pre-launch meeting** with the TTM and any additional WT members that the WTL wishes to involve. This pre-launch meeting marks the start of the test process. During the pre-launch meeting, the TTM briefs the target entity on the requirements for the TIBER-PT test process.

To facilitate the free, safe and secure flow of information, participating parties can sign Non-Disclosure Agreements (NDA).

After the pre-launch meeting, the target entity must start its procurement process for the RT provider and TIP. The entity shall conduct a due diligence process in line with its own existing risk management practices, to ensure that the selected TIP/RT provider meet all the requirements set out in the TIBER-EU Services Procurement Guidelines. Responsibility for ensuring that the appropriate TIP/RT provider are selected lays solely with the target entity. The target entity is also responsible for establishing the conditions that govern the sharing, confidentiality and retention of intellectual property rights. In the end of the procurement process, the WT must attest that, to the best of their knowledge, the procurement process adhered to both the relevant requirements in the TIBER-EU White Team Guidance[7] and the TIBER-EU Services Procurement Guidelines[8].

It should be noted that some providers provide both TTI and RT services, and target entities can opt to procure both services from the same provider.

Once the target entity has agreed the terms with the TTI and RT providers and completed the necessary contractual arrangements, the WT must produce the Project Plan, including the final schedule of meetings to be held between the target entity, TTI/RT providers and the TCT, and share this with all the relevant stakeholders.

The target entity shall hold a **launch meeting** and involve all the relevant stakeholders, to discuss the test process and their expectations, as well as the draft Project Plan. The launch meeting shall preferably be physically attended by all participants.

After the launch meeting, the WT and the TCT must agree on the low level scope of the RT test. The scope must include the target entity's CFs, but may also include non-critical functions at the target entity's discretion, provided that this inclusion does not negatively impact the testing of CFs.

[7] TIBER-EU White Team Guidance

[8] TIBER-EU Services Procurement Guidelines

As per the TIBER-EU framework, CFs are defined as "the people, processes and technologies required by the entity to deliver a core service which, if disrupted, could have a detrimental impact on financial stability, the entity's safety and soundness, the entity's customer base or the entity's market conduct". These CFs can also include the systems, people and business processes outsourced to third-party service providers.

Testing must be performed on the live production systems of the entity. However, the entity may also include other types of infrastructure, including pre-production, testing, backup and recovery systems, within the scope of the RT test.

Both the TCT and the WT should have extensive knowledge of the entity's business model, functions and services. Entities may conduct a business impact analysis to identify the CFs as part of their standard operational risk management practices. The TCT may, if it deems necessary, consult with the supervisors during this phase to ensure that all appropriate CFs are captured in the scope discussions.

The target entity must complete the TIBER-EU Scope Specification template[9], which shall frame the scope of the TIBER-PT test, and list the key systems and services that support each CF. This information shall be used by the WT to identify the targets and objectives that the RT must seek to achieve during the test. These targets and objectives are referred as "flags" and can be the achievement of certain levels of access, access to user credentials, access to sensitive data or other action(s) or indicator(s) of system compromise expected from the test actions.

The final TIBER-EU Scope Specification document shall be presented during a workshop (scoping meeting) organised by the entity for all relevant stakeholders, after discussions between the WT and the TCT and after the scope was formally agreed by the board of the target entity and the TCT. If the procurement has been completed before the scoping process the TIP and RT provider may be included in this process, at the WT's discretion.

The WT must discuss the flags with the TTM, who must approve them. The flags set during this process, can be changed on an iterative basis following the threat intelligence gathering and as the RT test evolves, with the agreement of the TTM.

In case the TIP/RT were not involved during the scoping process, the WT must ensure that a meeting is held with the providers after the scoping process to explain the CFs and systems that support them, to guarantee that these providers have an adequate knowledge of the entity before the start of the testing phase. Further dialogue is encouraged if the entity feels necessary to ensure the success of the test.

Prior to the test phase, the WT shall also conduct a risk assessment to ensure that the necessary

[9] TIBER-EU Scope Specification template

Risk management controls are in place. This includes, but is not limited to:

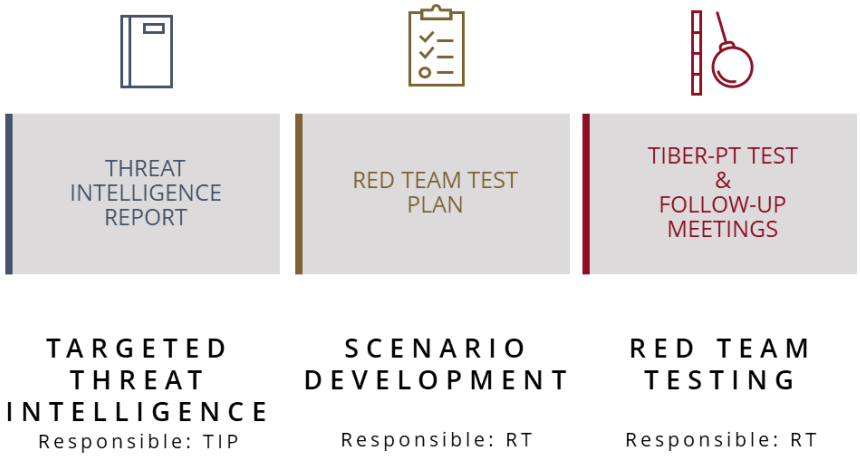
- in-scope systems prior to any testing should be part of the preparations to ensure that backup and restoration capabilities are in place and have been tested;
- protecting the confidentiality of the test via the use of NDA;
- clear escalation chains and contact persons for emergencies between the target entity and the external providers and within the target entity itself;
- clear mandate for the WT to order a halt to the tests in the event of heightened risk of damage and to determine the next course of action, in consultation with all relevant stakeholders;
- clear definition of actions that are out of bounds for the TIP and RT during the test;
- a written authorisation for the physical penetration (if applicable).

3.3 Testing Phase

During the testing phase, the TIP prepares a TTI Report on the target entity, setting out threat scenarios for the test and useful information on the entity. While preparing the TTI Report (if available, the GTL report shall be used as basis), the TIP works closely with the RT, assisted by the target entity, in the reconnaissance process, which consists of the collection of information about the target entity (people, technology, surroundings and environment) in preparation of a TIBER-PT test . The RT shall then use the TTI Report as the basis to develop attack scenarios and execute the TIBER-PT test in accordance with the approved scope.

The duration of the targeted threat intelligence and scenario development processes is approximately five to six weeks (that can be extended up to eight weeks if necessary and agreed with the TCT under a specific rationale) and the red team testing approximately 10 to 12 weeks.

Figure 3.3 • Overview of the Testing Phase.



3.3.2 Threat intelligence process

The targeted threat intelligence process main deliverable is the TTI Report, which shall give a detailed view of the target entity's digital presence, and take into consideration the real-life actors within the threat landscape, to help produce actionable and realistic attack scenarios. The development of the TTI Report is carried out by the TIP. The RT shall be involved towards the end of the phase, to review the TTI Report, and integrate the information into the Red Team Test Plan.

To make intelligence gathering as efficient and relevant as possible to the scope and to the entity's business, the target entity shall provide the TIP with a business and technical overview of each CF and supporting systems in scope, an up-to-date threat assessment and/or threat register and information from a sample of recent attacks. This information shall be provided using the TIBER-EU Guidance for Target Threat Intelligence Report[10]. Moreover, if the target entity possesses an internal threat intelligence function, the TIP should liaise with it and gather relevant information that will complement the TTI Report, if this can be done while preserving the confidential nature of the test. The use of various threat intelligence sources and methods by the TIP is encouraged.

During the targeted threat intelligence process, the TIP collects, analyses and disseminates critical function-focused intelligence relating to two key areas of interest:

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

To identify targets, the TIP should carry out an assessment similar to what threat actors partake when they prepare for their attack from outside the network, to obtain a preliminary picture of the entity and its weak points from the attacker's perspective. This shall result in the identification, on a critical function-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.

Threat assessment consists of an analysis by the TIP of the relevant threat actors and probable threat scenarios to gain insight into the cyber threat landscape, based on evidence-backed threat intelligence which is specifically tailored to the entity's business environment. This shall result in a summary of the key threats, detailed profiles of the threats with the highest scores, and potential scenarios in which a high-scoring threat actor might target the entity. This is a passive process, under no circumstances should active reconnaissance (direct engagement with target systems) be undertaken.

[10] TIBER-EU Guidance for Target Threat Intelligence Report

There are three outputs from the TTI Report that are particularly relevant for the design of the attack scenarios and red team test:

- tailored scenarios, which will support the formulation of a realistic and effective Red Team Test Plan;
- threat actor goals and motivations, which will help steer the RT in its attempt to capture the flags agreed upon in the scoping phase;
- validated evidence which will underpin the business case for post-test remediation and improvement.

Once the draft TTI Report is completed, the TIP should share it with the WT, the TTM and the RT for review, to check for factual errors and allow any issues to be discussed in a timely manner. This must occur no less than two weeks before the TTI and RT handover meeting (Section 3.3.3). Based on the TTI Report, the WT and TTM may also opt to update or modify the flags.

Due to the confidential nature of the TTI Report, all stakeholders must take the necessary precautions to protect its contents from leaking, both within and outside the entity.

3.3.3 Scenario development phase

Following completion of the targeted threat intelligence process, the RT takes the lead. Using the scenarios contained in the TTI Report, and in line with the TIBER-EU Test Scope Specification, the RT should develop and integrate the attack scenarios, based on real-life threat actors within a threat landscape, into a draft Red Team Test Plan. The scenarios are written from an attacker's point of view, and should result from a creative process, taking into account the target entity's maturity and security controls.

To ensure that the TIBER-PT test is adequately thorough, it is recommended that it includes physical red teaming in its scope, provided that the entity, and specifically the WTL can identify and manage appropriately the associated risk.

The attack scenarios are not a prescriptive playbook which must be followed precisely during the test and may be adjusted in the course of the test.

To facilitate a more effective and efficient test, the WT may deliver, at its discretion, additional information to the RT on the scenarios chosen, including on the people, processes and systems targeted in each scenario. This information may give the RT further insights and allow a better use of time. However, it should be evident that the information given to the RT could have been obtained by an advanced attacker with more time and unhindered by moral, ethical and legal constraints.

At this stage, a TI/RT handover workshop must be held involving all relevant stakeholders, namely the WT, the TTM and the TIP/RT. This meeting shall contemplate the following activities:

- the TIP presents an overview of the TTI Report;
- the WT and TCT provide feedback comments on the TTI Report;

• the RT presents the draft Red Team Test Plan, including CF scenario mapping, flags, possible anticipated leg-ups[11], risk mitigation, escalation procedures, test start/stop dates and a draft Red Team Test Report delivery date.

Following the workshop, the TIP should revise and produce a final version of the TTI Report for delivery to the entity, taking into account the feedback obtained during the workshop. Moreover, the RT shall similarly revise the draft Red Team Test Plan.

Due to the risk associated with a red team test, namely the degradation of services or disclosure of sensitive information that shall be avoided as much as possible, the RT shall include risk management controls in the test plan for managing these risks, and adjust the plan accordingly.

3.3.4 Red Team Testing

During the red team testing phase, the RT plans and executes a TIBER-PT intelligence-led red team test of the target systems and services that underpin each CF in scope. The time allocated to testing shall be proportionate to the scope and should approximately be 10-12 weeks.

The test objectives agreed during the scoping phase are the flags that the RT provider must attempt to capture during the test as it progresses through the scenarios.

Unlike the genuine threat actors, the RT is restricted by the time and resources available as well as by moral, ethical and legal boundaries, as such, it might be necessary for the WT to provide occasional leg-ups to help them progress (e.g. provide access to a system or internal network). The RT must make use of its creativity to develop alternative ways to reach the test objective or flag, when obstacles occur. If this is deemed unfeasible, and a leg-up is strictly necessary, the RT may request it to the WT. Should this happen, then the leg-up should be duly logged.

The TIP may provide ongoing threat intelligence to the RT during the test, to provide useful insight on how to achieve the targets. Where TIP and RT provider decide to work more closely during the test, the working arrangements and information sharing arrangements must be agreed between the two parties.

The TTM must be updated at least once a week by the RT provider. The way in which these updates shall occur must be agreed before the start of the test by both parties. The WT must also be informed of the progress of the tests on an ongoing basis. If feasible, physical meetings between the WT, TTM and RT provider during this phase are strongly encouraged, since the discussions add significantly to the quality of the test and help build a relationship of trust. However, any such

[11] Situations in which it may be necessary for the entity to give the RT access to its system, internal network, etc. to continue with the test and focus on the next flag/target.

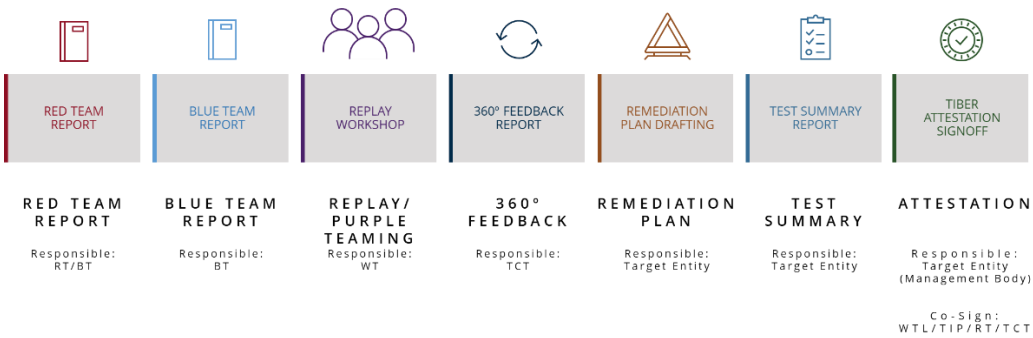
meeting should be conducted cautiously to ensure that the BT is not made aware of the ongoing test.

Whatever the methodology employed by the RT, the test shall always be conducted in a controlled manner, taking a stage-by-stage approach, as to avoid any significant impacts to the entity and its CFs. It is important for the WT and TTM to be continuously informed about progress being made at each stage, as soon as a flag or target is in sight, or at least when the RT has "captured the flag". These updates provide the WT with the opportunity to discuss with the RT and TTM what actions can and cannot be taken next. It also provides a chance for escalation procedures to be invoked where necessary. The WT can halt the test at any time if it considers necessary to do so. All of the RT's actions should be logged for the replay of the executed scenarios with the BT (i.e. review and discuss with the RT the steps taken by both parties during the test), as evidence for the Red Team Test Report, and for future reference.

3.4 Closure Phase

During the closure phase, the RT drafts the Red Team Test Report, which consists of the details of the approach taken to the testing and the findings and observations from the test. Where necessary, the report shall include advice on areas for improvement in terms of technical controls, policies and procedures, training and awareness. At this stage, the BT shall be made aware of the test, and shall also develop the Blue Team Report. Moreover, the BT shall be involved in the replay of the executed scenarios, to review and discuss with the RT the steps taken by both parties during the test (Purple Teaming exercise). The entity will take on board the findings, and will agree and finalise a Remediation Plan in close consultation with the TTM; the process of the test will be reviewed and discussed, resulting in a Test Summary Report elaborated by the BT and WT. Approval to close the test must be obtained from the relevant stakeholders (TIP, RT and TCT) once a Remediation Plan has been agreed. The closure phase takes approximately four weeks.

Figure 3.4 • Overview of the closing phase.



The RT is responsible for producing and delivering a draft Red Team Test Report to the entity within two weeks of test completion. The entity must then provide access to the document to the TCT for validation.

The key members of the BT are informed of the test and will use the Red Team Test Report to deliver the Blue Team Report. In the Blue Team Report, the BT maps its actions alongside the RT's actions. The Blue Team Report must be completed ahead of the replay workshop, within two to four weeks of the test completion.

The replay workshop must be arranged by the WT and should take place once both the Red Team Test Report and Blue Team Report are delivered. It shall serve as a learning experience to the relevant entity stakeholders, considering the insights obtained from testing, and with the assistance of the RT. During the workshop, a replay is organised in which the BT and the RT provider review the steps taken by both parties during the test (the TCT and TIP may also be present if they chose to). A purple teaming exercise, where the BT and RT collaborate to see what other steps could have been taken by the RT and what would be required of the BT to effectively respond.

The target entity may run, at its discretion, a purple teaming test, to augment the workshop and maximise the learning experience of the TIBER-PT test, as well as ensure that the remediation actions are appropriate and fit for purpose if the entity considers it appropriate. In such a case, the target entity must liaise with the TIBER-PT TCT to ensure its involvement, similarly to the test phase of the TIBER-PT test.

The TCT shall also arrange a 360-degree feedback workshop, where the entity, TCT, and TIP and RT should come together to review the test. In this meeting, all parties shall deliver feedback on each other and on the overall process, so that this feedback can be incorporated as a learning experience for all involved and for future exercises. The key topics to be covered, from all parties' perspectives, are:

- which activities/deliverables progressed well;
- which activities/deliverables could have been improved;
- which aspects of the TIBER-PT process worked well;
- which aspects of the TIBER-PT process could be improved;
- feedback on the TIBE-EU framework and supplementary guidance;
- any other feedback.

The TCT may share the output from the 360-degree feedback on an anonymous basis with the ECB's TIBER Knowledge Centre (TKC) so that all lessons learned can be reflected on and improvements can be made to the TIBER-EU framework and supplementary guidance. This is a key part of the "learning and evolving" principle that underlies the TIBER-EU framework. The main conclusions from this workshop shall be delivered in written form, in the shape of a 360-degree report.

The 360-degree feedback workshop is followed by the drafting of the Remediation Plan and Test Summary Report.

Based on the test results, the target entity shall design a Remediation Plan, which shall be used as basis for the implementation of the controls and improvements necessary to adequately solve or mitigate the vulnerabilities identified during the test.

The Test Summary Report summarises the overall test process and results (including the Remediation Plan) and should draw on the test documentation, such as the Red Team Test Report, the Blue Team Report, the TTI Report, the Red Team Test Plan and the Remediation Plan. The entity must share the Test Summary Report and Remediation Plan with the TIBER-PT authority's TCT (and other TIBER-XX authorities' TCTs involved in the test). The Test Summary Report must not contain detailed technical information and findings regarding weaknesses and vulnerabilities, as those are highly sensitive and for the entity only. The TCT may also review the more detailed findings from the test if this is deemed necessary.

Once the reports and Remediation Plan have been agreed, the entity, TIP/RT provider, WTL and TCT shall sign an attestation confirming that the test was conducted in accordance with the core requirements of the TIBER-EU framework. The attestation can serve as a way of qualifying the test for mutual recognition among other relevant authorities.

At this stage, the TCT will notify the supervisory and oversight functions of BdP that the test ended, but will not share TIBER-PT test information or documentation. Any sharing of test information, results and/or remediation measures is entirely voluntary, and to be decided by the target entity. It is recommended that the supervisors be involved during the implementation of remediation measures, due to its importance and potential impacts on the business functions of the target entity.

It is important to note that privacy-related information (e.g. employees' private information) shall be left out of test reports under all circumstances.

4 Disclaimer

This document describes the implementation of TIBER-PT and transposes its core elements. The information contained in this document is for information purposes only and it does not constitute a legal or any other expert assessment. The sponsors and authors of this document do not accept any responsibility for any errors, omissions or misleading statements in this document, or for any loss that may arise from reliance on the information and opinions expressed in it.

Each target entity undergoing a TIBER-PT test is exclusively responsible and liable for the execution of the tasks attributed to it by this framework, including compliance with applicable laws and regulations, and for any unintended consequences originating from the execution of said tasks. The target entity shall remain responsible for the independent legal and expert assessment of the intended test projects and to take appropriate risk management measures. BdP shall not be liable for any damages arising from the use of this document or from the TIBER-PT tests conducted by entities.

5 Annex

Annex 1 • List of the main deliverables expected during a TIBER-PT test.

Phase	Deliverable	Responsible	Template
Preparation Phase	Project Plan	WT	n.a.
	Scope Specification	WT	TIBER-EU Scope Specification template Risk Management Template
Testing Phase	TTI Report	TIP	TIBER-EU Guidance for Target Threat Intelligence Report
	RT Test Plan	RT	TIBER-EU Guidance for the Red Team Test Plan
Closure Phase	RT Test Report	RT	TIBER-EU Guidance for the Red Team Test Report
	BT Test Report	BT	n.a.
	360° Feedback Report	WT, TCT, RT, TIP	360° Feedback Report Template
	Remediation Plan	WT	n.a.
	Test Summary Report	WT	Guidance for the TIBER-EU Test Summary Report
	TIBER-PT attestation	TCT,WT, RT,TIP	TIBER-EU Attestation Template

Annex 2 • Responsibility Matrix

	TARGET ENTITY			Providers		TIBER Authority
	WT	Mgmt. Body	BT	RT	TIP	TCT
Pre-Launch Meeting	C	I				R
Procurement of TTI/RT Providers	R	A		I	I	C
Project Plan	R			C	C	C
Pre-test risk assessment	R	A		I	I	C
Launch Meeting	R	A				C
Draft Scoping Document	R	A		I	I	C
Scoping Meeting	R	A		I	I	C
Threat Intelligence Report	A			C	R	C
Handover workshop	A			C	R	C
Red Team Test Plan	A			R	C	C
TIBER-PT Test	A			R		C
Red Team Report	A		C	R		I
Blue Team Report	A		R	C		I
Replay Workshop	R	A	C	C	C	I
360º Feedback Meeting	C		C	C	C	R
360º Feedback Report	C		C	C	C	R
Remediation Plan	R	A		C	C	I
Test Summary Report	R	A		C	C	C
TIBER Attestation	C	R		C	C	C

Annex 3 • List of Abbreviations

Abbreviations	Explanation
BdP	Banco de Portugal
BT	Blue Team
CFs	Critical Functions
EBA	European Banking Authority
ECB	European Central Bank
GTL	Generic Threat Landscape
NDA	Non-Disclosure Agreements
RT	Red Team
TCT	TIBER Cyber Team
TIBER	Threat Intelligence Based Ethical Red Teaming
TKC	TIBER Knowledge Centre
TTI	Targeted Threat Intelligence
TIP	Threat Intelligence provider
TTPs	Tactics, Techniques and Procedures
TTM	Team Test Manager
WT	White Team
WTL	White Team Lead