

# TIBER-ES IMPLEMENTATION GUIDE

## Threat Intelligence Based Ethical Red-Teaming - Spain

**TIBER-ES IMPLEMENTATION GUIDE**

**Threat Intelligence Based Ethical Red-Teaming - Spain**

**TIBER-ES IMPLEMENTATION GUIDE**  
**Threat Intelligence Based Ethical Red-Teaming - Spain**

January, 2022

# Contents

**Abbreviations** 5

**1 Introduction** 5

- 1.1 Background 5
- 1.2 What is TIBER-EU? 6
- 1.3 What is TIBER-ES? 7
- 1.4 Purpose of this guide 7
- 1.5 Introduction to the TIBER-ES process 8
- 1.6 Who is eligible for this type of testing? 8

**2 Stakeholders and their roles** 10

- 2.1 The role of participant authorities 10
- 2.2 Participants 10
  - 2.2.1 TIBER Cyber Team 10
  - 2.2.2 Entity being tested 11
  - 2.2.3 Providers 11

**3 The TIBER-ES test process** 13

- 3.1 Preparation 13
- 3.2 Testing 16
- 3.3 Closure 19

**4 Risk management** 22

**5 Test results and their use in financial supervision and oversight** 23

**Annex Responsibility matrix** 24

## Abbreviations

BT	Blue Team
BTTR	Blue Team Test Report
GTL	Generic Threat Landscape
RT	Red Team
RTTR	Red Team Test Report
TCT	TIBER Cyber Team
TI	Threat Intelligence
TKC	TIBER-EU Knowledge Centre
TLPT	Threat Led Penetration Testing
TTI	Targeted Threat Intelligence
TTM	Team Test Manager
TTP	Tactics, Techniques and Procedures
WT	White Team
WTL	White Team Lead

## 1 Introduction

Technology is a key element in allowing financial institutions<sup>1</sup> to offer their services in a reliable and safe way that is consistent with their strategy and business model. Factors such as the high level of interconnectedness within the financial sector and with third parties, the continuous and rapid development of technology, the growing number and sophistication of cyber threats, the digitalisation of financial transactions and remote working have made entities' cyber resilience and cyber security a priority both from prudential and financial stability angles.

In this setting, entities' most vulnerable points may be subject to attacks that can sometimes be highly complex. Therefore, it is paramount that entities reduce their vulnerabilities and have in place an effective and mature cyber security control environment. However, this approach will only be successful if it allows them to effectively confront a real cyber attack.

In that sense, Threat Led Penetration Testing (TLPT) or intelligence-led red teaming tests aim to anticipate, insofar as possible, the impact that a real cyber attack could have on an entity. In order to do so, in this type of advanced cyber security testing, cyber attacks are simulated using the Tactics, Techniques and Procedures (TTP) that a sophisticated attacker would use. Accordingly, these tests constitute a very powerful tool to improve entities' cyber resilience.

### 1.1 Background

In 2016 the Bank of England published the first red teaming framework for the financial sector, CBEST.<sup>2</sup> In the same vein, in 2017 the Netherlands published the TIBER-NL<sup>3</sup> (Threat Intelligence

<sup>1</sup> For the purposes of this guide, the term "entity" will be used for simplicity, referring not only to any entity, institution or organisation that provides financial services to clients or members but also to the financial market infrastructures needed to provide those services.  
<sup>2</sup> <https://www.bankofengland.co.uk/-/media/boe/files/financial-stability/financial-sector-continuity/cbest-implementation-guide>.  
<sup>3</sup> <https://www.dnb.nl/media/1mdf3lmq/tiber-nl-guide.pdf>.

Based Ethical Red-teaming) framework, drawing on CBEST but with its own characteristics. Different jurisdictions around the world have also expressed their intention to develop local red teaming testing frameworks.

In this setting, in May 2018 the European Central Bank (ECB) published TIBER-EU, its own advanced cyber security testing framework, aiming to avoid fragmentation, standardise and harmonise these tests in Europe, prevent the emergence of non-compatible frameworks and save entities operating in multiple jurisdictions from unnecessary duplication of effort. Any jurisdiction may adopt TIBER-EU and draft its own implementation guide based on the framework.

## 1.2 What is TIBER-EU?

TIBER-EU is the first common European framework for intelligence-led red teaming testing. It describes the way in which authorities, entities and cyber security service providers should work together to achieve the goal of red teaming tests: that the entities being tested identify areas of improvement in their cyber resilience, not only in the technology field but also in people and procedure-related aspects.<sup>4</sup>

Although initially created for financial institutions and infrastructures, TIBER-EU may be adopted for application to any kind of entity in any sector.

The framework has been designed for its adoption by a lead authority that will be responsible for monitoring the execution of the tests and certifying their alignment with the requirements of the framework. Compliance with TIBER-EU's mandatory requirements allows mutual recognition of the tests among the different lead authorities that have adopted the framework locally.

The goal of the framework is not to assess test results as a pass or fail, but rather to improve the entity's knowledge of its own weaknesses and strengths when confronted with a cyber attack, and identify measures to enhance its cyber resilience.

Undergoing a red teaming test in accordance with the spirit and requirements of the TIBER-EU framework entails an inherent risk, given that they have to be performed on production environments.<sup>5</sup> Additionally, the framework requires that these tests be carried out by external providers, in order to ensure that the conditions of a cyber attack are simulated as realistically as possible, which makes the tests expensive. The costs and risks associated with these tests are assumed in all cases by the entities being tested and under no circumstances by the authorities adopting the framework.

One distinctive characteristic of the TIBER-EU tests, when compared with other cyber security tests,

---

4 A sophisticated cyber attack against the entity is simulated. In order to assess its protection, detection and response capabilities, only a very small group of staff should be aware of the test.

5 Production environments encompass the information technology systems in which the applications that provide services to end users, be they the entity's own employees or its clients, are executed and/or where processes use and produce real data and information.

is their holistic approach based on cyber intelligence. This enables entities to test their cyber resilience against real threats and weaknesses that are relevant for the financial sector, rather than basing the tests purely on the threats and weaknesses perceived or identified by the entities themselves.

### 1.3 What is TIBER-ES?

In December 2020 the Executive Commission of the Banco de España approved the adoption of the TIBER-EU framework, taking ownership of the national framework, assisted by the National Securities Market Commission (CNMV) and the Directorate General of Insurance and Pension Funds (DGSFP) where the entities to be tested come under their respective fields of competence.

The national framework – TIBER-ES – essentially aims to strengthen the cyber resilience of entities operating in Spain. The framework is to be implemented from a financial stability perspective and participation in these tests is voluntary for entities (see section 1.6, “Who is eligible for this type of testing?”).

TIBER-ES follows the principles of TIBER-EU, thereby ensuring that tests conducted under the local framework will be recognised by authorities in other jurisdictions which have also adopted TIBER-EU locally. To this end, it observes, inter alia, the requirement that the tests be conducted on production environments and executed by external third-party providers (their role is described in detail in section 2, “Stakeholders and their roles”). All costs and risks associated with the process are assumed entirely by the entities being tested.

TIBER-ES has been tailored for use across the entire financial sector.

### 1.4 Purpose of this guide

This implementation guide is part of the TIBER-ES framework and has been developed by the TIBER Cyber Team (TCT) led by the Banco de España, in close cooperation with the CNMV and the DGSFP.

The purpose of the document is to specify the conditions for the execution of red teaming tests under TIBER-ES requirements. The fundamental concepts and basic principles of the TIBER-EU framework are included in detail and the tests must comply with them. Apart from those requirements, the document is intended as a guide rather than a prescriptive inventory of activities.

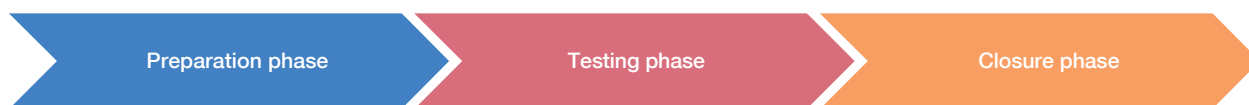
This document must be read along with the TIBER-EU framework and its accompanying documents published by the ECB, inter alia, the TIBER-EU Services Procurement Guidelines and the TIBER-EU White Team Guidance. All references to documents and templates published by the ECB included in this guide can be found on the TIBER-EU website.<sup>6</sup>

---

<sup>6</sup> <https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html>.

Figure 1

## THE TIBER-ES TEST PROCESS



SOURCE: TIBER Cyber Team.

Entities and Threat Intelligence (TI) or Red Team (RT) service providers may contact the TCT – via its mailbox, [tiberes@bde.es](mailto:tiberes@bde.es) – for clarification of any doubt about this document or the processes it describes.

### 1.5 Introduction to the TIBER-ES process

The main phases of a red teaming test under the TIBER-ES framework, aligned with those described in TIBER-EU, are described briefly below. A detailed description of the process is included in section 3, “The TIBER-ES test process”.

The TIBER-ES process is structured around three key phases:

- **Preparation.** The scope of the test is defined (focusing on critical business functions) and the teams responsible for managing it are established. The TI and RT providers are also selected.
- **Testing.** The TI provider will draft a report on the entity being tested. This will be the basis for preparing the attack scenarios. The RT provider will use these attack scenarios in its approach, aiming to compromise the entity’s production information systems, processes or people within the scope of the test. Successful compromise will be attested by achieving the targets set or capturing the agreed flags.
- **Closure.** The RT provider will draft a test report, including details of the process, recommendations for improvement and observations. The entity’s defensive security teams will be involved in this phase of the test and will analyse the results of the RT, being able to qualify or rerun certain parts of the scenarios in a replay. The entity will draft a test summary report and a remediation plan for implementation of the recommendations for improvement agreed.

### 1.6 Who is eligible for this type of testing?

Considering that the main goal of the TIBER-ES framework is to strengthen the cyber resilience of entities operating in Spain and contribute to the stability of the Spanish financial sector, the framework is particularly relevant for the most significant or systemic institutions. In particular, large banks, insurers and asset managers, as well as critical financial market infrastructures.



Although any entity may ask to undergo a red teaming test, the sophistication of these tests makes them advisable only for systemic entities or those that have achieved a certain level of cyber resilience maturity. Less mature entities will possibly have weaknesses that can be detected via simpler tests that entail lower costs and risks. The TCT will consider these circumstances when deciding whether to accept or deny test requests. In any event, TIBER-ES seeks to act as an effective catalyst, aiming to raise cyber security capabilities at all entities so as to make them eligible for this type of testing.

## 2 Stakeholders and their roles

### 2.1 The role of participant authorities

The Banco de España is the owner of TIBER-ES. It is therefore responsible for the development and maintenance of the TIBER-ES framework, of which this document is part. These functions will be performed through the TCT, comprising the Banco de España, CNMV and DGSFP. Coordination of the TCT's actions will lie with the authority under whose remit the entity being tested falls.

Within the remit of the TCT, teams will be assigned to monitor the complete execution of the red teaming tests under TIBER-ES, attest that those tests are conducted in accordance with the framework's requirements and ensure compliance with the TIBER-EU principles. In addition to the Banco de España, these teams will also include CNMV and DGSFP when the entities to be tested come under their respective fields of competence.

### 2.2 Participants

#### 2.2.1 TIBER Cyber Team

The Banco de España is responsible for establishing the governance structure of TIBER-ES. This includes coordinating the TCT for the definition and operational management of TIBER-ES.

In general, the TCT is responsible, inter alia, for the following functions:

- Periodically reviewing the TIBER-ES framework, applying lessons learned from its implementation and tests executed and, where appropriate, proposing updates for approval by the competent body of the Banco de España.
- Participating in the ECB's TIBER Knowledge Centre (TKC) and proposing adaptations to the TIBER-ES framework in accordance with the TKC's directions. This is the common forum where authorities from all the jurisdictions that have adopted TIBER collaborate and cooperate in the implementation and update of the TIBER-EU framework and its guidance.
- Invalidating tests that are not executed in accordance with TIBER-ES and TIBER-EU requirements.

The TCT does not play a supervisory role and its actions are not linked to the imposition of any requirements if weaknesses are found when executing the tests. Nor is it responsible for the actions undertaken by the entity being tested or its providers, or for the risks derived from the test.

For each red teaming test executed under TIBER-ES, the TCT will appoint from among its members a Team Test Manager (TTM) with relevant experience in the sector, both in cyber

resilience and project management. The TTM's responsibility is confined to the test for which he/she is appointed. The TTM must:

- Monitor the test to ensure that it complies with TIBER-ES and TIBER-EU requirements.
- Represent the TCT and coordinate its test support tasks throughout all the phases, acting as the point of contact between the different participants involved. The parts of the process where the TTM's participation is needed are specified in section 3, "The TIBER-ES test process".

## 2.2.2 Entity being tested

### White Team

For each test, the entity being tested has to establish a White Team (WT) which is ultimately responsible for defining the scope of the test and its effective execution. The WT will also have the power to withdraw from the execution of the test at any time, provided there are objective circumstances warranting it. The WT should have only a small number of members who must keep the test confidential, not informing any other divisions or areas of the entity. The WT's composition may vary in accordance with the phase and progression of the test.

The WT will be in charge of managing risks during the test and will comprise executive and management staff at the entity, including cyber security experts and those responsible for cyber incident escalation and notification processes.

A White Team Lead (WTL) will be appointed, from within the entity, to be responsible for the WT. The WTL will coordinate all the test-related activities with all the stakeholders, including providers.

Requirements for its composition, activities and responsibilities are described in the TIBER-EU White Team Guidance published by the ECB.

### Blue Team

The Blue Team (BT) will comprise all staff at the entity who are not part of the WT, in particular those managing people, processes and systems to be tested. The BT should not be aware of the execution of the test until the closure phase, when it will be able to participate in the replay and the follow-up of any remedial actions.

## 2.2.3 Providers

Before the tests are executed, the entity must agree with the providers involved at least on significant aspects, such as: pricing, the planned scope of the tests, the limits on execution and activities not allowed during the tests, the duration of the contract, the resources to be used by

the provider, the actions to be taken during execution of the tests, and the responsibilities to be assumed by the parties, including taking out insurance if needed.

It is crucial that providers and their staff are sufficiently independent of the entity being tested, to ensure the objectivity of the test results. They must also have enough credited experience and skills for the proper and safe execution of the tests.

A single provider may perform TI and RT functions simultaneously. However, these functions should be assigned to separate providers if a single provider cannot guarantee sufficient appropriate technical and human resources in the corresponding teams.

The requirements in terms of independence, experience and agreements with providers are described in the TIBER-EU Services Procurement Guidelines published by the ECB.

### **Threat Intelligence**

The Threat Intelligence (TI) provider is an external provider engaged by the entity. It will collect information, imitating the investigation that a cyber threat actor would conduct, and will provide the entity to be tested with a cyber intelligence report on specific threats, including potential real world cyber attack scenarios that could be executed by real world cyber threat actors. The provider should use multiple and updated sources of information.

### **Red Team**

The Red Team (RT) is a team provided by an external provider and engaged by the entity. Its goal is to compromise the entity's security capabilities using TTP and ethical hacking methods. It will execute its attacks based on the information provided and scenarios designed by the TI provider. At the end of the test, the RT will draft a report detailing how the scenarios were executed and describing the weaknesses found.

### 3 The TIBER-ES test process

This section describes in detail the main phases of a TIBER-ES test. Following the model established in TIBER-EU, each TIBER-ES test consists of three mandatory phases, each of which are subdivided into steps.

#### 3.1 Preparation

This phase starts once the entity to be tested and the TCT agree on the performance of the test. The TIBER-ES test is formally launched and the TCT starts liaising with the participating entity. This phase lasts approximately four to six weeks, not including the duration of the institution’s provider procurement process.

It consists of the following steps:

##### 1 Pre-launch:

- The entity will designate a WTL and establish the WT, the composition of which must be validated by the TTM. To this end, both the entity and the TTM will use the TIBER-EU White Team Guidance published by the ECB as a guide. The WT will be responsible for the overall management of the test (its role is described in detail in section 2, “Stakeholders and their roles”, and in the abovementioned ECB guidance).
- A pre-launch meeting will be held at which the TTM will brief the WT on the test process and characteristics, as detailed in this TIBER-ES Guide. More specifically, the briefing will address the requirements as to the stakeholders’ roles and responsibilities, the security and confidentiality protocols to be used (including those for secure document transfer and exchange), and preliminary test planning.
- The WT will adopt all necessary measures for management of the risks associated with the test, to ensure that it is conducted in a controlled manner and according to the entity’s risk appetite (see section 4, “Risk management”).

Figure 2  
**PREPARATION PHASE**



SOURCE: TIBER Cyber Team.

## 2 Procurement:

- The WT will start the process to identify potential TI and RT providers. Even if the entity is already performing red teaming using its internal TI and/or RT teams, the TCT will only consider a test as being in accordance with TIBER-ES if it is performed by external third-party providers. These third parties need to be independent of the entity and its BT in order to ensure the objectivity of the results and due confidentiality during the test. The external providers need to demonstrate sufficient previous experience in this type of tests and the appropriate technical skills and expertise for the safe and sound execution of the tests.

Throughout this process, the WT shall follow the requirements and principles contained in the TIBER-EU Services Procurement Guidelines published by the ECB.

- The entity will commence the procurement process, assess the providers' proposals and proceed to award the services.
- Arrangements between the entity and the providers will be formalised in contracts, including aspects such as pricing, the scope of the tests, the limits on their execution and activities not allowed, the duration of the contract, the resources to be used by the provider, the actions to be taken during the execution of the tests and the responsibilities to be assumed by the parties, including taking out insurance policies where necessary. They will also cover non-disclosure, confidentiality and data destruction requirements and early disclosure to the entity of any critical vulnerability detected during the execution of the tests.

Table 1

### PREPARATION PHASE

Goal	Deliverable or outcome	Responsibility	Validation
WT establishment	– WT established	Entidad	TTM
Pre-launch	– Pre-launch meeting – Preliminary test planning	WT	
Risk management	– Preliminary risk assessment – Risk mitigation/transfer measures defined WT	WT	
TI and RT procurement	– Invitations to tender, assessment of tender responses, award – Confidentiality clauses with TI and RT providers – Contracts with selected TI and RT providers – Cyber insurance taken out (optional)	WT	
Launch	– Test planning – Launch meeting – Progress timeline – Control points and deliverables	WT	
Scope and goals definition	– Scope definition meeting – Preliminary scope document – Scope document	WT	TCT TI/RT Provider Board

SOURCE: TIBER Cyber Team.

Given that formalisation of contracts generally requires a lengthy negotiation process, the subsequent steps of the preparation phase may be executed during the formalisation, provided that confidentiality arrangements among stakeholders are in place.

### 3 Launch:

- Once the TI and RT providers have been successfully selected, the WT will complete the test plan and the schedule of meetings to be held between the stakeholders.
- The WT will organise a launch meeting with the participation of TCT members and the TI and RT providers, to discuss the test process and the entity's expectations, test planning and a timeline, including meetings and checkpoints, as well as the documents and deliverables expected in each phase.

### 4 Scoping:

- The WT will define the preliminary scope of the test, which must include critical functions of the entity<sup>7</sup> and the systems and services underpinning and supporting them. Optionally, the WT may also include non-critical functions. Entities should use their internal analysis, such as Business Impact Analysis (BIA), to define their critical functions.

These critical functions may be completely or partially outsourced. In this case, the entity will assess the feasibility of including a representative of the third party to which the function is outsourced as a WT member. The ultimate goal is to conduct the test on the outsourced function in the same manner and with identical requirements as if it was not outsourced.

The WT will set on the systems and services underpinning the critical functions the targets or flags to be captured by the RT during the test. Nevertheless, these targets may be altered as the TI provider obtains new cyber intelligence and the RT executes the test. Although the test must be performed on live production systems, the targets may also include pre-production, testing and disaster recovery systems.

The TIBER-EU Scope Specification Template published by the ECB is recommended for drafting the preliminary scope document.

- The WT will share the preliminary scope document with the TCT and the TI and RT providers to incorporate their feedback. Accordingly, the TCT will need to have a broad knowledge of the entity's business model and its critical functions and services. Additionally, the TCT may consult the entity's supervisory or oversight authority, be it a national or a supranational one (for instance, the SSM Joint Supervisory Teams).

---

<sup>7</sup> According to the TIBER-ES framework, an entity's critical functions are defined as the people, processes and technologies it requires to deliver core services which, if disrupted, would have a detrimental impact on financial stability or on the entity's safety and soundness, customer base or market conduct. It is not a system but a business function essential to the sector or entity.

- The WT will organise a scoping meeting at which the preliminary scope document will be presented for validation by the TCT and the TI and RT providers.
- The WT will submit the preliminary scope document for formal approval and endorsement by the entity's board of directors. Once the scope document is approved, planning may be amended if necessary.

## 3.2 Testing

This phase comprises information gathering and drafting of a cyber intelligence report by the TI provider, and the definition of the plan for the test and its execution by the RT. It has an estimated duration of 16 to 18 weeks.

It consists of the following steps:

### 1 Threat intelligence gathering:

This step aims to simulate the information gathering prior to an attack that a real cyber threat actor would perform during the reconnaissance phase. The information obtained has to be relevant for the scope of the test as established in the previous phase (see section 3.1, "Preparation"). The information gathered will serve as a basis for preparing tailored attack scenarios that are feasible, meaningful and have a considerable impact on the targeted entity. During this first cyber intelligence step, it is important to reflect the main threats the entity may face and to obtain an overview of its exposure and defence mechanisms that is as complete as possible. This way, the TTPs that a real cyber threat actor would use can be imitated or employed. The estimated duration of this step is five weeks.

There are two mutually complementary cyber intelligence tools to produce the threat-based scenarios: the Generic Threat Landscape (GTL) report for the sector in which the entity operates, and the Targeted Threat Intelligence (TTI) report with the specific threats relevant for the entity undergoing the TIBER-ES test.

The GTL report for the financial sector is usually produced by specialised service providers or national cyber security and/or cyber intelligence agencies. Where available, it should be used as a basis for the drafting of the TTI.

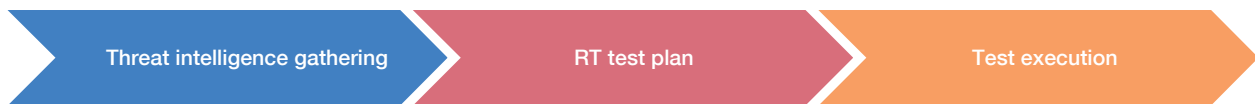
Therefore:

- The TCT will supply the entity's TI provider with the GTL report, where available.
- The TI provider will draft the TTI report. To that end, the TIBER-EU Guidance for Targeted Threat Intelligence Report published by the ECB can be used as a reference. To obtain the maximum added value for the test, it is strongly recommended that the entity supplies the TI provider with relevant information on the threats and vulnerabilities



Figure 3

**TESTING PHASE**



SOURCE: TIBER Cyber Team.

that a real cyber threat actor could exploit. The information delivered by the entity should be similar to that which a threat actor unconstrained by time limitations or by moral, ethical or legal boundaries could obtain. The TI provider will also use its own resources to gather additional public or accidentally leaked information on the entity.

The TTI will include information on the systems supporting the critical functions, a list of threats to which the entity may be exposed, the cyber threat actors that could perpetrate attacks, examples of recent attacks and, lastly, probable attack scenarios. These scenarios should be realistic and useful for the test plan to be drafted by the RT and should include threat actor goals and motivations

- The TI provider will facilitate the draft TTI report to the WT, the RT and the TCT for their review.
- The WT will hold a specific meeting to validate the TTI. It is particularly important that the RT validates the threat scenarios defined, given that it is responsible for drawing up a test plan based on those scenarios. However, the TTI report may be updated while the RT’s test plan is being drafted, and even during the test, where necessary and if agreed by all stakeholders.

**2 RT test plan:**

The estimated duration of this step is one to two weeks.

- The RT will draft a test plan based on the TTI report. For that purpose, the TIBER-EU Guidance for the Red Team Test Plan, published by the ECB, can be used as reference. The test goals agreed during the scoping step, possibly updated during the TTI report drafting, will be the flags to be captured by the RT during the execution of the test.

Optionally, the entity could provide the RT with relevant information to better simulate the conditions of a real attack. The WT shall take the necessary measures to assist the RT as and when requested by the provider.

The RT test plan will comprise a series of scenarios representing concrete goals to be achieved. To define them, the RT will draw on the scenarios defined in the TTI report; it may, however,

include new scenarios deemed relevant, or a combination of existing scenarios. The RT should use its knowledge and experience, combining available internal cyber intelligence with open source information, to define alternatives within the original scenarios should the first attack option be unsuccessful.

- Once the TTI report and the RT test plan are completed, the WT will set up a meeting for the TI and RT providers to discuss operational details, with the participation of the TCT.

### 3 Test execution:

The time allocated for the RT's task should be in keeping with the defined scope and with the WT's and RT's capacity and resources. A time frame for the execution of the RT test is between 10 and 12 weeks.

As of that moment, the RT takes command of the execution of the test. The RT should develop alternative attack techniques in case it finds obstacles that prevent it from achieving the defined goals or from capturing the assigned flags.

The RT may sometimes ask the WT for assistance to disable internal barriers and/or security controls to expedite the test (a leg-up). One example of this would be allowing access to an internal network segment or system, in order to continue with the test and advance towards the next goal

Table 2

#### TESTING PHASE

Goal	Deliverable or outcome	Responsibility	Validation
Generic threat intelligence	– Delivery of the GTLR to the TI provider (optional)	TCT	
Specific threat intelligence	– Organisation's input to the drafting of the TTI, providing relevant information about threats and the vulnerabilities that could be used by a real attacker (optional)	WT	
	– Preliminary TTI report	TI Prov.	
	– TTI report validation meeting	WT	WT/TCT/RT
	– TTI report	TI Prov.	
Test plan and scenarios definition	– Organisations input to the test plan and realistic scenarios definition by the RT provider, consisting in information that might be used by a real attacker (optional)	WT	
	– RT's test plan	RT	
Pre-execution coordination	– TI and RT providers coordination meeting	WT	
RT test plan execution	– Executed actions log	RT	
	– Internal barriers and/or security controls disabled to expedite test (optional)	WT/RT	
Progress updates	– Regular test progress updates (at least weekly) to WT and TCT	RT	
Execution coordination	– Regular follow-up and coordination meetings between the RT providers, the TCT and the TW. Meetings could include the TI provider if deemed necessary (optional)	WT	

SOURCE: TIBER Cyber Team.

or flag. This may occur when the entity's BT successfully defends the goal or flag, or when time restrictions impact a process that both the WT and the RT deem as trivial and which a threat actor would successfully compromise given sufficient time. In the event the RT makes this kind of request and it is granted, this should be reflected in the reports since the outcome from the moment a security control or mechanism is disabled must be put into context.

The RT will keep the WT updated on progress at all times and should inform the TCT at least weekly on the progress made in the execution of the test. Where possible, meetings between the RT, the WT and the TCT are recommended during this step, including the TI provider if deemed necessary. These meetings add significant value to the test quality and help ensure trust between stakeholders. It is paramount that the BT is not aware of these meetings.

All actions of the RT must be logged so that the BT can replay them after the testing phase.

### 3.3 Closure

The closure phase allows all stakeholders to assess the outcome of the test and highlight the improvements needed to strengthen the entity's cyber resilience. Test reports are drafted in this phase, highlighting improvements regarding technical controls, policies, processes and procedures, as well as staff awareness and training. The executed plan is replayed and discussed with the BT, a remediation plan is defined, the outcome of the test is shared with the stakeholders and the attestation of the test confirming that it was performed in accordance with TIBER-ES requirements is signed. The estimated duration of this phase is four weeks.

This phase consists of the following steps:

#### 1 RT and BT report drafting:

- The RT will send a draft of the Red Team Test Report (RTTR) to the WT and the TCT no later than two weeks after the test is concluded. The draft should preferably be based on the TIBER-EU Guidance for the Red Team Test Report published by the ECB.
- The WT will inform the key members of the entity's BT of the test carried out. They will use the RTTR to draft their own Blue Team Test Report (BTTR). This report will link their actions to the RT's actions and must be completed before the replay of the RT test (see next step) to make the most of the lessons learned.

#### 2 Test replay, lessons learned and remediation plan:

- The test will be replayed by the RT and the BT and both will review the steps taken. To do so, the RT may use activity logs. It is not strictly necessary for the replay to be complete or for it to be made in production environments. The goal is to learn from the experience gained from the test, in cooperation with

Figure 4

**CLOSURE PHASE**



SOURCE: TIBER Cyber Team.

the RT provider. In addition, the RT should give its opinion on which goals a real attacker could have achieved, given more time or resources than those used in a TIBER-ES test.

- Optionally, a Purple Team can be created, from among the RT and the BT, to jointly assess which decisions could have been made by the RT during the test and how the BT would have responded to them.
- Afterwards, the WT will hold an evaluation meeting with all the stakeholders: the entity (represented by the WT), the TCT and the TI and RT providers. In this meeting lessons learned during the execution of the test will be assessed for their use in future tests. Additionally, views regarding other relevant aspects will be gathered to improve the TIBER-ES framework and this implementation guide.
- The entity should draft a remediation plan for implementation of the agreed recommendations for improvement. This plan, which should be agreed with the TI and RT providers and the TCT, will help implement improvements to mitigate or solve the weaknesses found during the test and improve the entity’s cyber resilience.
- The entity will send the remediation plan for implementation of the recommendations for improvement to its – national or supranational –supervisory or oversight authority.

**3. Test summary report:**

- The entity will draft a test summary report, based on documents such as the TTI report, the RT test plan, the RTTR and the BTTR and the remediation plan for implementation of the recommendations for improvement. This report will be drafted preferably using the Guidance for the TIBER-EU Test Summary Report published by the ECB. This report will not include detailed technical information on the weaknesses and vulnerabilities found, since that information is highly sensitive and is intended only for the entity. The report will be shared with the TCT, which may review the test conclusions in more detail if it deems necessary.

Table 3

**CLOSURE PHASE**

Goal	Deliverable or outcome	Responsibility	Validation
RT's conclusions	– RTTR sent to WT and TCT	RT	
Communication of the test to the BT	– The WT will brief key members of the BT on the test	WT	
BT's conclusions	– BTTR sent to WT and TCT	BT	
Test replay	– Test replayed in accordance with RT and BT criteria, both parties will review steps taken	RT/BT	
Analysis of lessons learned	– Purple Team created from among the RT and the BT (optional)	WT	
Evaluation	– Evaluation meeting and feedback from all stakeholders: WT, BT, TCT and TI and RT providers	WT	
Remediation plan	– Remediation plan for implementation of the recommendations for improvement	WT	TCT TI/RT Prov.
	– Remediation plan sent to supervisory authority	WT	
Test validation	– Validation and attestation of compliance with TIBER-ES requirements	WT TI/RT Prov. Board	TCT

**SOURCE:** TIBER Cyber Team.

- The entity will send the test summary report to its – national or supranational – supervisory or oversight authority.

**4. Test attestation:**

Upon completion of the test, after the remediation plan for implementation of the recommendations for improvement is agreed, the WT, the TI and RT providers and the TCT should validate that the test has been carried out in accordance with TIBER-ES requirements. The WT will attest to this with a document signed both by the entity's board of directors and the providers. This attestation, provided it is validated by the TCT, will allow the test to be mutually recognised by other jurisdictions that have adopted the TIBER-EU framework locally. The TIBER-EU Attestation Template published by the ECB should be used for this attestation.

## 4 Risk management

Risk management in tests undertaken under the TIBER-ES framework is of paramount importance, since these cyber resilience tests have to be flexible, realistic and conducted on production environments. This entails risks as to the confidentiality, integrity and availability of systems and data (including particularly sensitive data that may be protected by current regulations, such as personal data). Incorrect execution of these tests could damage systems and applications and cause system failures, as well as data alteration, data deletion or illicit data leaks.

First of all, it is key to identify and analyse in detail the risks that might materialise when executing the test and take appropriate measures to mitigate these risks, before, during and after the test. To this end, it is paramount to have a contingency plan. The WT is responsible for ensuring that risks associated with TIBER-ES tests are identified, analysed and mitigated at all times. The TCT will monitor the execution of the tests, but it will not be liable for any damage caused to entities as a result of their execution. Taking out cyber insurance is one way to complement risk mitigation with transfer strategies.

For these reasons, it is important that the chosen TI and RT providers meet the minimum requirements established in the TIBER-EU Services Procurement Guidelines. Contracts with providers should include confidentiality clauses and cover aspects such as security requirements, responsibilities, indemnification, limits on execution and activities that are not allowed during the test (for example, destruction of equipment or data, uncontrolled modification of data or programs, jeopardising the continuity of critical systems, extortion or threats to employees or disclosure of the test results).

As regards confidentiality during the execution of the tests, it must be ensured that nobody at the entity outside the WT is aware of the test. To that end, non-disclosure agreements may be signed with the providers.<sup>8</sup> Participants in the test should use code names for the entity being tested to protect its identity. The WT should manage the escalation of cyber incidents related to the test to avoid triggering responses that would be mandatory in the event of a real cyber incident, such as contacting third parties, including law enforcement. If the TTM suspects that the BT is aware of the test and is trying to manipulate its results, he/she may choose not to validate the test as being in accordance with TIBER-ES requirements.

---

<sup>8</sup> Under current legislation, confidential information or data shared by entities with authorities are subject to a duty of professional secrecy.

## 5 Test results and their use in financial supervision and oversight

Details of the outcome of a TIBER-ES test are the sole property of the entity being tested. For security reasons, the highly confidential nature of the information contained in reports like the RTTR or the BTTR advises against sharing them with third parties. This recommendation also applies to RT and TI providers and to the TCT, none of which should store or keep the entity's confidential information beyond the time required for the test.

The remediation plan for implementation of the recommendations for improvement and the test summary report are an exception to the above-mentioned limitations, since they will include no technical details, so that they may be shared with the supervisory or oversight authority and the TCT, and with any other party the entity deems appropriate. For more details, see section 3, "The TIBER-ES test process".

Additionally, the TCT may share with the TKC information from the remediation plan for implementation of the recommendations for improvement, for example, weaknesses detected or lessons learned. The information will be anonymised and will be exchanged in all cases through secure channels. This will allow the TKC to aggregate data on key common thematic areas to develop a picture of the current state of cyber resilience in the European financial sector.

As stated in the Introduction, the TIBER-ES framework is adopted from a financial stability perspective. Therefore, the team in charge of the regular supervision or oversight of the entity being tested will have limited implication in the test, being involved in very specific phases of the process:

- Preparation: for information purposes, the entity will inform the team in charge of its supervision or oversight that the execution of the TIBER-ES test has begun. Moreover, the TCT may ask the supervisory or oversight authority if the scope defined by the WT for the test covers critical functions of the entity.
- Closure: the entity will send the test summary report and the remediation plan for implementation of the recommendations for improvement to its supervisory or oversight authority.

## Annex Responsibility matrix

Table A.1

### PREPARATION PHASE

Goal	Deliverable or outcome	Responsibility	Validation
WT establishment	– WT established	Entidad	TTM
Pre-launch	– Pre-launch meeting – Preliminary test planning	WT	
Risk management	– Preliminary risk assessment – Risk mitigation/transfer measures defined WT	WT	
TI and RT procurement	– Invitations to tender, assessment of tender responses, award – Confidentiality clauses with TI and RT providers – Contracts with selected TI and RT providers – Cyber insurance taken out (optional)	WT	
Launch	– Test planning – Launch meeting – Progress timeline – Control points and deliverables	WT	
Scope and goals definition	– Scope definition meeting	WT	TCT
	– Preliminary scope document		TI/RT Provider
	– Scope document	WT	Board

SOURCE: TIBER Cyber Team.

Table A.2

### TESTING PHASE

Goal	Deliverable or outcome	Responsibility	Validation
Generic threat intelligence	– Delivery of the GTLR to the TI provider (optional)	TCT	
Specific threat intelligence	– Organisation's input to the drafting of the TTI, providing relevant information about threats and the vulnerabilities that could be used by a real attacker (optional)	WT	
	– Preliminary TTI report	TI Prov.	
	– TTI report validation meeting	WT	WT/TCT/RT
	– TTI report	TI Prov.	
Test plan and scenarios definition	– Organisations input to the test plan and realistic scenarios definition by the RT provider, consisting in information that might be used by a real attacker (optional)	WT	
	– RT's test plan	RT	
Pre-execution coordination	– TI and RT providers coordination meeting	WT	
RT test plan execution	– Executed actions log	RT	
	– Internal barriers and/or security controls disabled to expedite test (optional)	WT/RT	
Progress updates	– Regular test progress updates (at least weekly) to WT and TCT	RT	
Execution coordination	– Regular follow-up and coordination meetings between the RT providers, the TCT and the TW. Meetings could include the TI provider if deemed necessary (optional)	WT	

SOURCE: TIBER Cyber Team.



Table A.3

**CLOSURE PHASE**

Goal	Deliverable or outcome	Responsibility	Validation
RT's conclusions	– RTTR sent to WT and TCT	RT	
Communication of the test to the BT	– The WT will brief key members of the BT on the test	WT	
BT's conclusions	– BTTR sent to WT and TCT	BT	
Test replay	– Test replayed in accordance with RT and BT criteria, both parties will review steps taken	RT/BT	
Analysis of lessons learned	– Purple Team created from among the RT and the BT (optional)	WT	
Evaluation	– Evaluation meeting and feedback from all stakeholders: WT, BT, TCT and TI and RT providers	WT	
Remediation plan	– Remediation plan for implementation of the recommendations for improvement	WT	TCT TI/RT Prov.
	– Remediation plan sent to supervisory authority	WT	
Test validation	– Validation and attestation of compliance with TIBER-ES requirements	WT TI/RT Prov. Board	TCT

**SOURCE:** TIBER Cyber Team.

BANCO DE ESPAÑA  
Eurosystem



GOBIERNO  
DE ESPAÑA

VICEPRESIDENCIA  
PRIMERA DEL GOBIERNO  
MINISTERIO  
DE ASUNTOS ECONÓMICOS  
Y TRANSFORMACIÓN DIGITAL

SECRETARÍA DE ESTADO  
DE ECONOMÍA  
Y EMPRESA  
DIRECCIÓN GENERAL  
DE SERVICIOS  
Y FONDOS DE PENSIONES

CNMV  
COMISIÓN  
NACIONAL  
DEL MERCADO  
DE VALORES