

TIBER-FR NATIONAL IMPLEMENTATION GUIDE

How to implement TIBER-EU
and DORA TLPT
in financial institutions
under French jurisdiction

VERSION 2

TABLE OF CONTENTS

1. INTRODUCTION TO TIBER-EU

2. HOW DOES TIBER-EU RELATE TO DORA TLPT?

3. TIBER-FR OVERVIEW

4. RISK MANAGEMENT FOR TIBER-FR TEST AND CONFIDENTIALITY

5. MAIN STAKEHOLDERS IN A TIBER-FR TEST

5.1. Test management actors

5.1.1. Roles and responsibilities of the test management actors

5.2. Test implementation actors

5.2.1. Role and responsibilities of the Threat Intelligence provider

5.2.2. Role and responsibilities of the Red Team provider

5.2.3. Purple Teaming

6. TIBER-FR PROCESS

6.1. The preparation phase

6.1.1. Procurement of Threat Intelligence and Red Team services

6.2. The testing phase

6.2.1. The Threat Intelligence sub-phase

6.2.2. The Red Teaming sub-phase

6.3. The closure phase

6.3.1. Blue Team Report

6.3.2. Replay workshop and Purple teaming exercise

6.3.3. Test Summary Report

6.3.4. 360° Feedback Workshop

6.3.5. TIBER-FR attestation

LIST OF ACRONYMS

ACPR	Autorité de Contrôle Prudentiel et de Résolution (French Prudential Supervisory Authority)
AMF	Autorité des Marchés Financiers (French Financial Markets Authority)
ANSSI	Agence National de Sécurité des Systèmes d'Information (French National Cyber Security Agency)
BT	Blue Team
BdF	Banque de France (French Central Bank)
CF	Critical Function
CI	Concerned Institution (Entity undergoing a TIBER-FR test)
CT	Control Team
CTL	Control Team Lead
DORA	Digital Operational Resilience Act
ECB	European Central Bank
EU	European Union
FMI	Financial Market Infrastructure
GTL	Generic Threat Landscape
HUMINT	Human Intelligence
OSINT	Open-Source Intelligence
PT	Purple Teaming
RACI	Responsible Accountable Consulted Informed (RACI-Matrix)
RT	Red team
RTT	Red team testers (preferably external testers but under certain conditions internal testers can be allowed)
RTS	Regulatory Technical Standards
RTTP	Red Team Test Plan
SGDSN	Secrétariat Général de la Défense et de la Sécurité Nationale (General Secretariat for Defence and National Security)
SSM	Single Supervisory Mechanism
TECHINT	Technical Intelligence
TI	Threat Intelligence
TIP	Threat Intelligence provider
TIBER-EU	Threat Intelligence Based Ethical Red Teaming Europe
TCT-FR	TLPT/TIBER Cyber Team France
TLPT	Threat Lead Penetration Testing
TPM	TIBER Program Manager
TTI	Targeted Threat Intelligence
TM	Test Manager
TTPs	Tactics, Techniques and Procedures

LEGAL DISCLAIMER AND COPYRIGHT NOTICE

This document provides a framework for recommendations and best practices. It does not create any legally binding obligations, nor supersede any international or domestic laws, regulations or requirements applicable in France. It should neither be relied upon nor treated as a substitute for specific advice relevant to particular circumstances.

This document, the "TIBER-FR implementation guide", is compliant with and based on the [TIBER-EU framework](#) and on the Delegated Regulation supplementing the Regulation (EU) 2022/2554 on digital operational resilience for the financial sector with regard to regulatory technical standards on Threat Led Penetration Tests (TLPT). This guide also incorporates specific content from other TIBER-XX implementation guides, such as valuable return on experiment.

The TIBER-FR implementation guide does not apply to credit institutions classified as "*Significant Institutions*" by the Single Supervisory Mechanism (SSM) where the European Central Bank is the competent TLPT authority under DORA regulation.

© Banque de France, 31 rue Croix-des-Petits-Champs 75001 PARIS, <https://www.banque-france.fr/>.

All rights reserved. Reproduction for educational and non-commercial purposes is permitted provided that the source is acknowledged.

4

PURPOSE OF THIS GUIDE

The present TIBER-FR implementation guide (hereafter referred to as "the Guide") aims at incorporating specific features required by French national laws into the [TIBER-EU framework](#). Unless specifically stated in this guide, [TIBER-EU framework](#) principles remain unchanged and applicable in TIBER-FR. Moreover, this guide reflects the return on experiment from the TCT-FR and other TCTs as part of a continuous improvement approach. This document is not a detailed prescriptive method and should be consulted alongside other TIBER-FR and TIBER-EU materials provided by the TCT-FR.

The TCT-FR is available to answer any questions that financial entities or external cybersecurity service providers might have concerning the methodology. Questions can be submitted to tiber-fr@banque-france.fr.

PREREQUISITES

We recommend that readers consult TIBER-EU framework document in addition to the TIBER-FR guide, as they are complementary. The TIBER-FR guide does not provide an in-depth description of all notions taken from the TIBER-EU framework where they have already been thoroughly presented.

Other TIBER-EU guidance materials provide useful recommendations and best practices for organizing a TIBER test and will be mentioned in the present guide:

- [TIBER-EU Framework Services Procurement Guidelines](#) provide more information on the process of selecting and procuring the services of threat intelligence and red-team providers;
- [TIBER-EU Control Team Guidance](#) explains how to set up the team which manages the TIBER test from inside the target entity;
- [TIBER-EU Purple-Teaming Best Practices](#) provide guidance on how purple-teaming may be introduced and managed in the TIBER testing phase and/or closure phase as outlined in the TIBER-EU framework.

1. INTRODUCTION TO TIBER-EU

The Framework for Threat Intelligence-Based Ethical Red Teaming (TIBER-EU) comprises a set of recommendations (best practices) which enable European and national authorities to collaborate, on a voluntary basis (or when applicable on a mandatory way to fulfil DORA TLPT legal requirements), with financial institutions (hereafter referred to as “entities”), to put in place a program to test and improve their resilience against sophisticated cyber-attacks.

TIBER-EU is a common framework that delivers a controlled, bespoke, intelligence-led red team test of entities’ critical live production systems. It allows the tested entities to understand their real-world resilience by testing the critical or important functions of their business against the tactics, techniques and procedures (TTPs) of the actual threat actors that are specific to their organisation. The intelligence-led red team test provides a comprehensive end-to-end understanding of weaknesses present in people, business processing, technology, and their associated intersection points, and provides a detailed threat assessment which can be used to further enhance the entity’s situational awareness.

The idea of TIBER-EU is to:

- Bring together the best available governmental and/or commercial threat intelligence, tailored to the business model and operations of a particular entity, and to set up credible scenarios mimicking the key potential attackers and the attack types they could deploy;
- Use this intelligence to enable ethical red team testers to simulate more accurately, and in a controlled manner, real-life attacks from competent adversaries on the live production systems of the entity.

5

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

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

Intelligence-led red team tests mimic the TTPs of advanced threat actors who are perceived by threat intelligence as posing a genuine threat to entities.

An intelligence-led red team test involves the use of a variety of techniques to simulate an attack – either by malicious outsiders or by staff – on an entity’s information security arrangements (i.e. its people, processes and technologies). The test helps an entity to assess its protection, detection and response capabilities.

2. HOW DOES TIBER-EU RELATE TO DORA TLPT?

Regulation (EU) 2022/2554 on the digital operational resilience of the financial sector (known as DORA) provides in its Article 26 for the mandatory exercise of advanced penetration testing (known as TLPT) on financial entities identified as critical or having a potential systemic impact. In France, these entities are designated by their respective TLPT Authorities, i.e. the Banque de France, the ACPR or the AMF. In the case of credit institutions classified as “*Significant Institutions*” the TLPT Authority is the ECB.

DORA regulation requires a Threat Led Penetration Testing (TLPT) framework inter alia, in accordance with TIBER-EU. The TIBER-EU framework as well as TIBER-FR implementation should thus be seen as compliant with DORA TLPT

requirements and providing additional operational guidance. DORA and the Delegated Regulation on Threat Led Penetration Tests represent the legal specification of what needs to be done or achieved during a test in order to be compliant (the “WHAT”) while the TIBER-EU framework (and TIBER-FR) provides a methodological support on how TLPT should be operationalised both by the tested entity and by the TLPT authority (the “HOW”).

In this guide, both advanced penetration testing required by DORA regulation, and TIBER tests, are referred as Threat Led Penetration Tests, or using the acronym TLPT, as considered similar in terms of methodology and requirements.

3. TIBER-EU OVERVIEW

TIBER-FR is the implementation of the TIBER-EU framework for France, incorporating specific national features.

TIBER-FR is used by the French TLPT authorities as operational framework both to conduct mandatory advanced penetration tests under DORA when applicable (or under any other regulation enforcing such testing) or to perform voluntary threat intelligence based ethical red-teaming under TIBER-EU.

Both DORA regulation and TIBER-EU require TLPT authorities to set up a TLPT Cyber Team (TCT) in charge of ensuring that TLPT requirements are properly applied by the entities undergoing a test. In order to ensure a consistent approach for the French financial sector and to benefit from synergies, in particular on entities supervised by several national competent authorities, the Banque de France, the ACPR and the AMF decided to set up **a common team at national level : the TCT-FR** (without prejudice to the competence of each TLPT authority).

A TIBER-FR test is generally performed within a 3-year cycle; to be noted that this duration can be shortened or extended based on the competent TLPT authority appreciation. The test is recognised in all EU jurisdictions that have implemented TIBER-EU when the tested entity operates its business on a cross-border basis, with a presence in multiple EU jurisdictions (mutual recognition).

After designation by their TLPT authority (formal letter of identification is sent), entities are notified by the TCT-FR of the start date of their mandatory DORA TLPT (letter of notification is sent). Entities which are not required to perform mandatory DORA TLPT can be invited by the TCT-FR to perform a voluntary TIBER-FR test. In both cases, the TIBER-FR guide will be used as operational framework. During the test, the external Threat Intelligence provider (TIP) and the Red Team Testers (RTT) - preferably an external provider but internal testers can be allowed under certain conditions - identify and simulate the most relevant threats to the tested entities' critical functions, mimicking TTPs of existing highly skilled threat groups. As such, the prevention, detection and response capabilities of the tested entities against these kinds of attacks are assessed (capability assessment).

The Concerned Institution (entity undergoing a test - CI) is the owner of the TIBER-FR test, while the TCT-FR accompanies the CI during the entire test and ensures the requirements are properly applied. TIBER-FR engagements require resources (human and financial supplied by the CI), involve multiple stakeholders over a few months, demanding from the CI thorough planning and coordination between all test participants.

A TIBER-FR test requires the involvement of the following main actors:

- the TIBER/TLPT Cyber Team (TCT-FR) and Test Managers (TM) Lead and Alternate
The TCT-FR ensures the test is conducted by the CT in accordance with the requirements of the TIBER-FR implementation guide (which fulfills DORA requirements). The TM Lead is the main point of contact for the CI and collaborates closely with the CTL during the test (the TM Alternate takes over the TM Lead role in case of vacancy to ensure the continuity of the test).
- the Control Team (CT) and Control Team Lead (CTL)
The CI sets up a CT led by the CTL who is responsible for conducting the end-to-end test and ensuring that all risk management controls are in place to facilitate a controlled test.
- the Blue Team (BT)
Comprises all staff at the CI in charge of security and response capability. It is critical that the BT remains completely excluded from the preparation and conduct of the test.
- the Threat Intelligence provider (TIP)
External supplier responsible for defining threat scenarios aimed at mimicking potential threat actors' attacks against the live systems that underpin the critical functions of the CI.
- the Red Team Testers (RTT)
External supplier or internal testers (subject to approval by the TM) in charge of simulating a real-life and realistic attack on the CI's live systems based on the threat scenarios defined by the TIP.

7

TIBER-FR sets out a three-phase process for an end-to-end test as follows:

- ❶ The **preparation phase** – During this phase, the following takes place: the engagement for the TIBER-FR test is formally launched; the team responsible for managing the test is set up; **the scope of the test is determined, approved and attested by the entity's board, and validated by the TCT-FR**; and the TIP and RTT are procured to carry out the test.
- ❷ The **testing phase** (which includes threat intelligence and red teaming)
 - The **TI sub-phase** – The procured TI provider prepares a Targeted Threat Intelligence Report (TTI Report) on the CI, setting out threat scenarios for the test and useful information on the entity.
 - The **RT sub-phase** – The TTI Report will be used by the RTT to develop attack scenarios and execute an intelligence-led red team test of specified critical live production systems, people and processes that underpin the tested entity's CFs.
- ❸ The **Closure phase** – During this phase, the RTT drafts a Red Team Test Report, which will include details of the testing approach and the test findings and observations. Where necessary, the report will include advice on areas for improvement in terms of technical controls, policies and procedures, and education and awareness. The main stakeholders will now be aware of the test, and should replay the executed scenarios and discuss the issues discovered during the test. The CI will take on board the findings, and will agree and finalise a Remediation Plan; the testing process will be reviewed and discussed; and the key findings from the test will be shared with the TCT-FR.

4. RISK MANAGEMENT FOR TIBER-FR TEST AND CONFIDENTIALITY

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

Therefore, prior to commencing any testing activity, the CT is required to conduct an in-depth risk assessment, in line with the entity's existing risk management framework, followed by the implementation of all the necessary risk mitigating controls, processes, and procedures to ensure a controlled test.

To further limit the risks incurred when conducting a TIBER-FR test, the TIBER-FR national implementation guidelines prohibits certain specific testing activities. These activities include:

- Destruction of equipment;
- Uncontrolled modification of data / programs;
- Jeopardising continuity of critical services;
- Extortion;
- Threatening or bribing employees;
- Disclosure of results.

8

The testing activities performed by the RT must of course be in accordance with the applicable legislation and the rules of engagement agreed upon by all participants.

The tested entity shall remain responsible for the independent legal and expert assessment of the intended TIBER-FR test. The Banque de France, the ACPR and the AMF shall not be liable for any damage arising from the use of the TIBER-FR implementation guide nor from the TIBER-FR test activities conducted under the sole responsibility of the tested entity.

Any person having access to Confidential Information is subject to the obligation of confidentiality. Any Confidential Information received in the context of a TIBER-FR engagement will be disclosed on a need-to-know basis only to persons involved in that test and provided that such persons are subject to the same obligations of confidentiality. Upon the conclusion or termination of the TIBER-FR engagement, the TIP and RTT will promptly (and no later than 3 days after such termination), either deliver all Confidential Information in tangible form (including any copies thereof) then in their possession to the tested entity's Control Team Lead (CTL), and certify in writing that all such Confidential Information has been destroyed. All Confidential Information shall be deleted from the systems and records. Notwithstanding the foregoing, a participant may retain copies of the Confidential Information for the purposes of, and for as long as required by any applicable laws or regulations.

"Confidential Information" means all information communicated to any person involved in the test, in any form and regardless of whether it is marked or otherwise identified as confidential, including but not limited to ideas, formulae, compositions, processes, procedures and techniques, research and development information, computer program codes, performance specifications, support documentation, drawings, specifications, designs and personal data.

Each participant shall process personal data solely for the purposes of executing the TIBER-FR engagement and in accordance with applicable laws, regulations, and Government instruction manuals, circulars and circular minutes on data management.

"Personal data" include surnames, first names, business email addresses and information that identifies the representatives of each participant.

5. MAIN STAKEHOLDERS IN A TIBER-FR TEST

The main stakeholders that may be involved in a TIBER-FR test are:

BDF, ACPR, AMF	TESTED ENTITY		PROVIDERS (OR INTERNAL RTT)	
TLPT CYBER TEAM (TCT-FR)	CONTROL TEAM (CT)	BLUE TEAM (BT)	THREAT INTELLIGENCE (TIP)	RED TEAM (RTT)
Ensures that the tested entity undertakes the test in a uniform and controlled manner, and in accordance with the TIBER-FR.	Is responsible for the overall planning and management of the test.	Comprises all staff in charge of security and response capability. It is critical that the BT remains completely excluded from the preparation and conduct of the test.	Defines threat scenarios aimed at mimicking potential threat actors' attacks against the live systems that underpin the critical functions of the tested entity.	Simulates a real-life and realistic attack on the tested entity's live systems based on the threat scenarios defined by the TI.
TEST MANAGER (TM)	CONTROL TEAM LEAD (CTL)			

Source: TCT-FR.

The TCT-FR is under the operational responsibility of the TIBER Program Manager (TPM). The TPM coordinates the governance activities overseeing the different TIBER-FR engagements, the transversal activities and (inter)national fora and committees to which the TIBER-FR team contributes. The TPM is also the first escalation point in case of issue or incident during a specific engagement, and thus is kept informed of the status of the different engagements by the Test Managers (TM).

For further information on the description, role and responsibilities of the different stakeholders, refer to the [TIBER-EU framework](#) here a RACI matrix is available in Table 5.

In case of a multi-jurisdictional TIBER/DORA test, the TLPT authority of the tested entity informs the TLPT authorities in host member States and assesses their respective willingness to be involved in the engagement, how they are to be involved and in what capacity, depending on the coverage and location of the tested critical functions¹ (CFs).

To structure the rest of this chapter we will distinguish between Test management actors and Test implementation actors.

5.1. Test management actors

The two key stakeholders involved in managing the test are the CT within the tested entity and the TCT-FR. Both the TCT-FR and CT should have extensive knowledge of the entity's business model, functions and services.

The Control Team (CT) and Control Team Lead (CTL): For each TIBER-FR test, the tested entity needs to form a CT with a dedicated CTL. The CTL coordinates all test activities including engagement with the TIP and RTT and meetings with the TCT-FR. All staff who are not part of the Control Team (CT) should be left unaware of the TIBER-FR test. Especially, **it is crucial that the Blue Team** ("BT"), which comprises all staff in charge of security and response

^① Within 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". Note that a CF is not a system. It is a function which could be considered critical or essential to the financial services sector and/or a financial services sector organisation.

capability, **remains completely excluded from the preparation and conduct of the TIBER-FR test**. More details on the roles, responsibilities and ideal composition of the CT can be found in the [TIBER-EU Control Team Guidance](#).

The TIBER/TLPT Cyber Team France (TCT-FR) and Test Managers (TM) Lead and Alternate: For each TIBER-FR test, the TCT-FR names at least 2 people: a TM Lead and a TM alternate, with experience in the relevant sector, as well as cyber expertise and project management skills. The role of the TM is to make sure that the entity undertakes the test in a uniform and controlled manner, and in accordance with the TIBER-FR mandatory requirements (which are in line with DORA TLPT requirements). The TM reports operationally to the TPM during the test. The role of the TM alternate is to take over TM Lead role in case of vacancy to ensure continuity of the test.

5.1.1. Roles and responsibilities of the test management actors

All parties involved in a TIBER-FR test should take a collaborative, transparent and flexible approach to the work. Close cooperation between the CTL and TM is required during all phases of the test.

The end-to-end conduct of a TIBER-FR test is the responsibility of the CI, which is responsible for the overall planning and management of the test. The TCT-FR, and subsequently the TM, is independent from the CT and is not accountable for the CT's actions, the conduct of the test, the outcomes or the remediation planning. It is the responsibility of the CT to ensure that a fit and proper test is conducted in line with the TIBER-FR guide, and therefore with DORA TLPT requirements, and that risks are managed throughout all phases.

10 The CTL is responsible for defining the scope, the scenarios and risk management controls for the test, ensuring that they have been approved by its governing body and validated by the TCT-FR. To validate the scope, the TCT-FR consults the relevant supervisory team² within the TLPT authority (or authorities in case of a co-supervised entity) to ensure it is appropriate for the test to begin. Then the TM ensures that the test is executed according to the plan and that it conforms to TIBER-FR test standards and all mandatory TIBER-EU requirements (as set out in Annex I of the [TIBER-EU framework document](#)) in order to ensure that a test attestation can be issued in the end (see section 5.3.5 below).

The CTL should coordinate all test activities including engagement with the TIP and the RTT. The CTL should ensure that the TIP/RTT's project plans are factored into the entity's overall project planning for the TIBER-FR test. If there are significant deviations in the original planning, this should be discussed with the TM. Although the CTL is the primary contact for the TIP/RTT, the TM should also have direct access to the providers (or internal testers) when required.

It is critical that all relevant stakeholders keep each other informed at all stages to ensure that the test runs smoothly and that any blocking factors, constraints, difficulties, deviations from the plan etc. can be addressed in a timely manner. When there are crucial decisions to be made (e.g. deviations during the test from the agreed scope), the CTL and TM should have a formal escalation line to their respective superiors.

² Supervisory teams are only consulted to verify that the scope defined by the CT is complete. They will not be involved in the remainder of the TIBER-FR engagement.

5.2. Test implementation actors

Within an end-to-end TIBER-FR test, there are two key actors that have a role in its execution: **the TIP and RTT**. In case of external RTT, it can be 2 different service providers for TI and RT activities or the same provider can cover both. In any case, the contractual relationship is agreed between them and the CI (Refer to § 5.1.1).

5.2.1. Role and responsibilities of the Threat Intelligence provider (TIP)

TIBER-EU defines threat intelligence as *“information on relevant threat actors and probable threat scenarios”*. Threat intelligence encompasses: (1) technical details like indicators of compromise (the “what”, “when” and “where”); TTPs of threat actors (the modus operandi or the “how”); and (3) the profile of the attackers themselves and their motivations (the “who” and “why”).

Creating accurate and realistic threat intelligence is a complex activity. This means that the TI provider must have adequate knowledge of the threat actors, their motives and their skills and TTPs, as well as an understanding of how the core elements of the financial system interact and operate. In addition, the TI provider must be able to acquire a good insight into the targeted entity. It needs to know for example: what the target’s critical functions are; how the target operates; who the (crucial) employees are and whether they are “usable” for the attack; and what the target’s vulnerabilities are.

The TI provider delivers threat intelligence to the tested entity in the form of a TTIR Report (TTIR).

The TI provider should use multiple sources of intelligence to provide an assessment that is as accurate and up to date as possible. The TTIR sets out the threat scenarios that can be used by the RTT to develop attack scenarios for the red team test.

The TI provider must demonstrate willingness and the ability to share its deliverables (once approved by the CT) with its Red Team testing counterpart for review and comment and demonstrate a willingness to work with the RTT during the remainder of the TIBER-FR test. This includes helping to develop the attack scenarios for the red team test, as well as any new intelligence requirements that come to light as the red team test progresses. The TI provider may have to update the TTIR in the course of the test and must be ready to do so.

Further information on drafting the TTIR is provided in the [TIBER-EU guidance for the Target Threat Intelligence report \(TTIR\)](#).

5.2.2. Role and responsibilities of the Red Team testers (RTT)

As a reminder, RT testers are preferably external but internal testers can be allowed under certain conditions and upon approval of the TM.

The RTT plans and executes a TIBER-FR test of the target systems and services, which are agreed in the scope, based on the threat scenarios in the TTIR and their conversion into attack scenarios in the Red Team Test Plan. This is followed by a review of the test and any issues arising, culminating in **a Red Team Test Report drafted by the RTT**.

The RTT should expand on and execute the established threat scenarios identified by the TI provider and approved by the CT and TM. The threat scenarios are developed from real attackers’ point of view. The RTT 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 changing circumstances or in case used attack methods do not succeed during the test. The scenario development is a creative process, and TTPs should not simply mimic scenarios seen in the past but should look to combine the TTPs of various relevant threat actors. The RTT should aim to assess the cyber resilience posture of the entity in the light of the specific threat it faces (or a scenario X can be considered as described in § 6.2.1).

The RTT apply a rigorous and ethical red team testing methodology, and must meet the minimum requirements defined under the TIBER-EU framework and in the TIBER-EU Service Procurement Guidelines. The rules of engagement and specific testing requirements should be established by the RTT and the tested entity.

The RTT must demonstrate a willingness to work closely with the TI provider, which includes reviewing and commenting on the intelligence deliverables (once approved by the entity) as well as transforming threat scenarios into a cohesive and tractable Red Team Test Plan. Furthermore, the RTT are expected to liaise and work with the TI provider throughout the testing in order to update the threat intelligence assessment and attack scenarios with relevant and up-to-date intelligence. The RTT may need to update the Red Team Test Plan during the course of the test and must be ready to do so. Lastly, the RTT are expected to work with the TI provider in order to design and deliver the final report issued to the entity.

5.2.3. Purple Teaming

Purple teaming is defined as an activity whereby both RT and BT are aware the test is taking place.

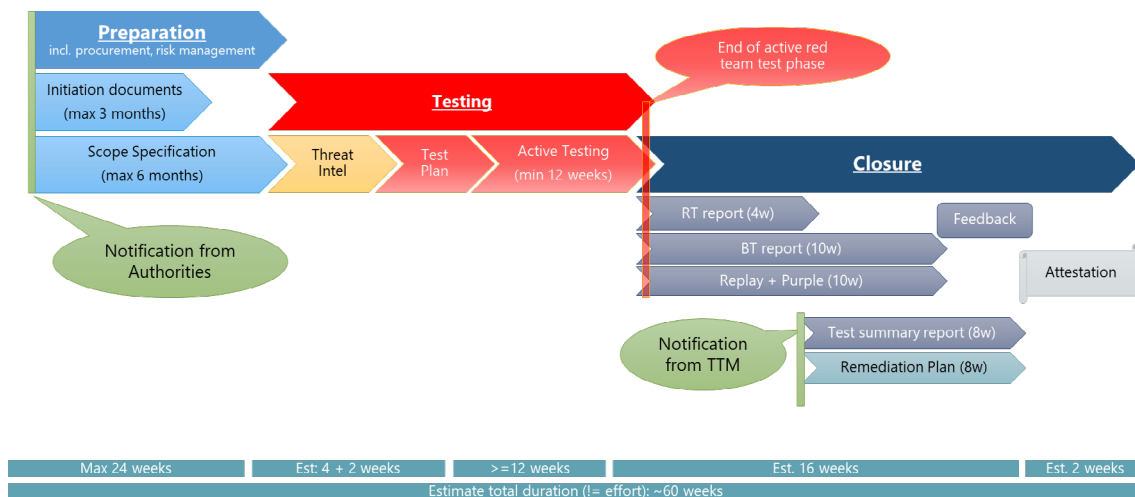
In practice, purple teaming may be implemented as part of the active Red Teaming as a measure of last resort when RT activities are detected by the BT in order to complete the current testing scenario (the secrecy of the other scenarios must be preserved as much as possible).

During the closure phase (after the completion of the replay exercise), a PT exercise is conducted as a mandatory requirement, in which the RT and the BT come together to discuss all remaining or additional topics relevant to the CT and the BT. This exercise is highly beneficial for increasing the learning experience of the entity, anchoring the learnings of the test within the organisation. Potential topics for the PT exercise should be jointly identified by the CT, RTT and the BT and could range from a table-top discussion to technical walkthroughs of the systems. The PT exercise must take place within ten weeks after the end of the active testing.

Further guidance and information about Purple Teaming is provided in [TIBER-EU Purple-Teaming Best Practices](#).

6. TIBER-FR PROCESS

A TIBER-FR test is generally performed within a 3-year cycle; to be noted that this duration can be shortened or extended based on the competent TLPT authority appreciation. The test is recognised in all EU jurisdictions that have implemented TIBER-EU (and have to comply with DORA), when the tested entity operates its business on a cross-border basis, with a presence in multiple EU jurisdictions (mutual recognition).



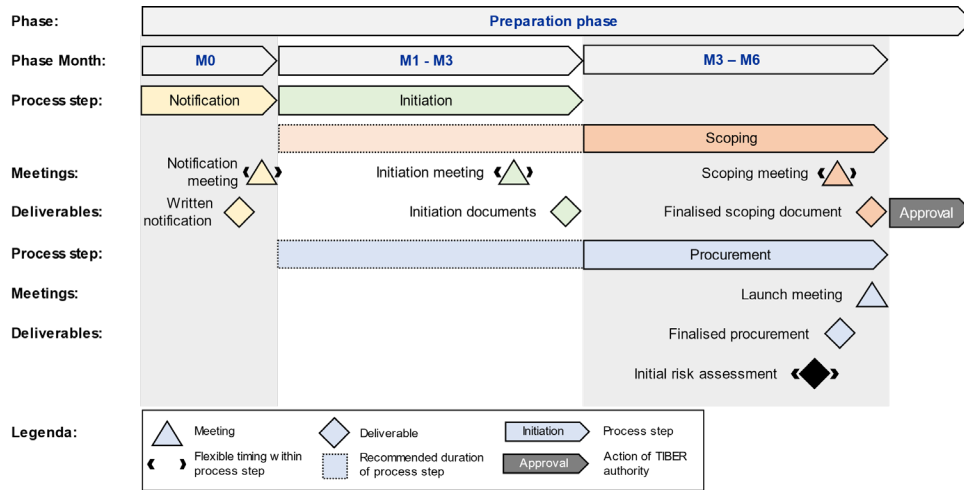
13

A preliminary step consists in drafting a Generic Threat Landscape (GTL) document, which is provided by the TCT-FR. The GTL is a generic assessment of the French national financial sector threat landscape, outlining the specific activities of the financial institutions, identifying the relevant high-end threat actors for the sector and the TTPs targeting these entities. The GTL will link these threat actors and the TTPs to the specific entities within the sector. The GTL Report aims to provide TI providers with a base of information and analysis, which can then be used to produce more entity-specific TTI Reports.

TIBER-FR sets out a three-phase process for an end-to-end test as follow.

6.1. The preparation phase (which includes Engagement & Scoping, and TIP/RTT procurement)

During the preparation phase, the engagement is formally launched. The scope is established, and the tested entity procures TI and RT services. **The duration of the preparation phase is 6 months maximum.**



Source: TIBER-EU.

14

Following the Notification meeting, regular status update meetings between the TCT-FR and the CT are held to check on preparation progress and assist the CT where needed.

Inputs of the phase	Outputs of the phase
TIBER-EU Control Team Guidance	The tested entity's Control Team is formed, including the appointment of a CTL, and all stakeholders are identified.
TIBER-EU Services Procurement Guidelines	TI and RT service provider(s) procured by the tested entity.
Scoping Specification Guidelines and scope attestation Template	Analysis produced by the tested entity, checking compliance with TIBER-EU Services Procurement Guidelines for both of the procured service provider(s).
Risk Management Guidelines	Scope Specifications produced by the Tested entity for review and approval by the TCT. Scope (including flags) is approved by a senior executive or board member (by signing a dedicated attestation). This senior executive or board member will sponsor the TIBER-FR engagement and ensure board awareness and buy-in for the engagement and the remediation of any findings that may be detected during the assessment.
	Risk management documentation produced by the tested entity (the TCT is consulted). Once approved, Scope Specifications and Risk management documentation are shared with the TIP and the RTT.
	High level Project Plan produced by the Tested entity for validation by the TCT-FR and aligned with the TIP and RTT.

6.1.1. Procurement of Threat Intelligence and Red Team services

To ensure a controlled and safe test, one prescribed control in TIBER-FR is the **use of specialist external** Threat Intelligence (TI) and Red Team (RT) providers, which have the highest level of skills and expertise, and have the requisite experience in threat intelligence and red team testing in the financial services industry to be able to deliver effective and cutting-edge professional services. External providers provide a fresh and independent perspective and are likely to have more resources and up-to-date skills to deploy, which would add value to the tested entity. To be noted that internal testers are allowed under certain circumstances, while the TI is always external.

Prior to engagement with potential TI and RT providers with a view to performing a TIBER-FR test, **the tested entity has to take into consideration the requirements of TIBER-EU Services Procurement Guidelines. The TM is consulted by the CT during the procurement process and can object to the choice of providers selected by the tested entity (or can object to the choice of internal testers if applicable).**

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

A single provider may fulfil both TI and RT roles in a TIBER-FR test. However, during the procurement process, the CTL must require guarantees that the provider can supply sufficient and qualified human resources in both the corresponding TI and RT teams. Moreover, **the TI and RT teams must remain independent from each other** so that the RT does not influence the reporting of the TI.

15

6.1.2. Regulatory security requirements

Entities which test and improve their resilience against sophisticated cyber-attacks have to take into account security requirements in accordance with both EU regulations and French specific laws.

Firstly, the Directive (EU) 2016/1148 dated 6 July 2016, recalling that “reliability and security of network and information systems and service are essential to economic and societal activities”, confirmed that its measures do not affect the Eurosystem’s oversight regime of payment and settlement systems, as required by the ECB in its opinion of 25 July 2014. The French law 2018-133 dated 26 February 2018 (article 2) recalled that EU supervisory procedures (requests for information and documents, general investigations, on-site inspections) keep their priority, in accordance with the monitoring authorities missions.

Secondly, entities must nevertheless take into account further obligations related to the State fundamental interests. In particular, French law defined two main classifications for private or public entities:

- the **Information Systems of Vital Importance** (SIV) operated by « Critical National Institution» (Opérateur d’Importance Vitale - OIV) (law 2013-1168 dated 18 December 2013, article 22, known as “loi de programmation militaire” or « LPM », article L. 1332-1 of French Defence Code),
- the **Operators offering Essential Services** (“OSE”) to the functioning of society or the economy and whose continuity could be seriously affected by incidents affecting the networks and information systems (law 2018-133 dated 26 February 2018, article 5).

Thirdly, considering that the French Prime Minister sets the security rules necessary for the protection of the information systems of the operators mentioned above, the French National Cyber Security Agency (ANSSI), managed by the

Secrétariat Général de la Défense et de la Sécurité Nationale (SGDSN - General Secretariat for Defence and National Security), a department dealing with global security issues, currently defines procedures in compliance with the legislation in force. Hence the entity must check its situation and take measures to mitigate any risk arising from any potential conflict of law (Regulation (EU) 795/2014, article 3).

Quarterly, the security elements and classified parameters delimited by the Regulation (EU) 2018/151, implementing Directive (EU) 2016/1148, and the French decree PRMD1630722A of 28 November 2016 setting the security rules and procedures relating to the sector of activity "Finance" may be used in good faith by the entity. As a result, in the context of a TIBER-FR test, shall the CT of the OIV entity decide to set flag(s) on SIIV systems, a formal list of certified suppliers in charge of auditing SIIV systems published by the ANSSI, known as the PASSI LPM, enables the entity to fulfill security requirements (classified information, processes, documents, computerized data or files). Moreover, the selected TI and RT providers are not allowed to delegate the work to sub-contractors which are not PASSI LPM certified and are not based in the EU. Similarly to a SIIV audit, the tested entity has no obligation to address the TIBER-FR report to the ANSSI but must be able to provide it to the ANSSI on demand.

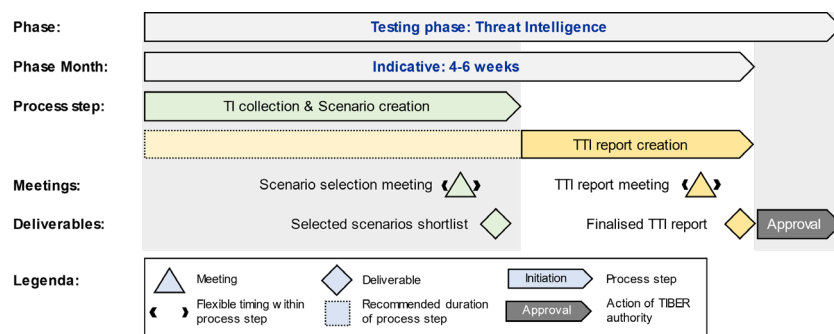
In addition, if no flags are set on SIIV systems by the CT of the OIV entity then it is only recommended to select TI and RT providers which are PASSI-RGS certified and are based in the EU.

6.2. The testing phase (which includes TI and RT activities)

16

6.2.1. The Threat Intelligence (TI) sub-phase

The procured TI provider prepares a **Targeted Threat Intelligence Report (TTI Report)** on the entity, setting out threat scenarios for the TIBER-FR test.



Source: TIBER-EU.

Inputs of the phase	Outputs of the phase
Scope specifications	The TI provider delivers a Target Threat Intelligence Report (TTIR).
Generic Threat Landscape (GTL) document	
TIBER-EU guidance for the Target Threat Intelligence report (TTIR)	
Intelligence collection input for the TI provider (provided by the CT)	

During the TI phase, the selected provider goes through four main stages as described below.



Source: TCT-FR.

6.2.1.1. Step 1: Targeted Intelligence collection

In this part of the TI phase, the TI provider executes an initial, furtive, broad, and intelligence-based targeting exercise of the kind typically undertaken by threat actors as they prepare for their campaign.

Active reconnaissance on the CI is not part of the Targeted Threat Intelligence phase so as to minimise the risk of detection before the Red Team phase has even started. The focus is therefore on stealth, using passive reconnaissance techniques with the objective of depicting the CI as a target from the attacker's perspective.

The main input for this part of the Threat Intelligence phase is the scoping document drafted by the CT, defining the Critical Functions and underlying systems that will be the target of the TIBER-FR engagement. Besides this scoping information, the use of various methods (including OSINT, TECHINT, HUMINT and intelligence-based initial targeting) is expected.

After receiving the scoping document, the TI provider is expected to request additional information from the CT to assist in intelligence collection and avoid going off scope. This can for instance be a list of domains or IPs in scope, but can also be additional information regarding business processes and entities in scope (offices, data centres, group companies, specific geographies, etc.).

The output of the Target Intelligence identifies the people, processes, technology and infrastructure of the tested entity on a Critical Function-focused system-by-system basis, including any critical third-party providers supporting these critical functions. This includes information that is publicly available about the institution, as well as internal information that has been deliberately or unintentionally leaked. This can include customer data, confidential material, identified vulnerabilities or other information that could prove to be useful for an attacker.

6.2.1.2. Step 2: Threat actors mapping

In this part of the TI phase, the different malicious cyber actors posing a threat to the CI will be investigated and categorized. The TI provider will identify the threat actors most relevant to the tested entity and map the TTPs attributed to these threat actors. This threat intelligence work builds on the GTL given to the TI provider at the start of the threat intelligence phase. **The TI provider is expected to enrich the information provided in the GTL document** with its own insights and the intelligence collected in the Targeted Intelligence collection step to produce a contextualised report representing the targeted threat landscape for the CI and its critical functions. Any relevant development that occurred after the creation of the GTL should also be taken into account.

6.2.1.3. Step 3: Threat Intelligence-based scenarios

Once a thorough investigation of the threat landscape is performed, the TI provider will develop several realistic scenarios. These scenarios are specifically tailored to the CI and aim to emulate the threat actors posing the greatest threat to the institution. For each scenario, the TI provider will define the narrative, the likelihood, the impacted Critical Function and supporting systems, corresponding flags, the involved threat actor to be emulated, the TTPs used by the selected threat actor, and the potential impact on the financial sector, etc.

The TI provider is also expected to include any of the identified target intelligence that could make scenarios even more tailored to the CI or be useful to the Red Team when executing them. The narrative of the scenarios should not limit the creativity of the RT too much as real Threat Actors demonstrate flexibility and also adapt their TTPs in an opportunistic manner. As such, the CT and TCT-FR rely on the professional judgement of the RT and TI providers to suggest alternative TTPs that the RT could use (provided the emulated Threat Actor is deemed to possess the ability to use these TTPs) in case of issues identified or anticipated with the TTPs prescribed in the scenarios.

Under TIBER-FR national implementation guidelines, the TI provider may consider a physical breach scenario. In such a scenario, the Red Team would be expected to bypass the on-premises physical security measures (e.g. by means of social engineering) to achieve a specific goal described in the scenario (e.g. install a malicious implant, steal confidential information...). A physical breach scenario is optional and may be decided by the CT to exclude it from the proposed scenarios in agreement with the TCT-FR.

Once the TI provider has a first draft of the scenarios it plans to include in the TTI report, a TI midpoint workshop is organised. During the workshop, the TI provider will present the different relevant scenarios it has identified and request input from the different participants in the engagement (CT, TCT-FR, if considered relevant by the TM then the RTT can start to be involved)

6.2.1.4. Step 3: (Optional) Scenario X

18

At most, one of the selected scenarios may be based on a forward-looking and potentially fictive threat actor with high predictive, opportunistic or prospective value given the anticipated developments of the threat landscape faced by the CI. This scenario X may deviate from the threat intelligence and employ TTPs not usually employed by the identified threat actors, or simulate a combination of different actors.

Given that only known and observed TTPs are used in the threat intelligence-based scenarios, more mature institutions have often already mitigated the vulnerabilities, rendering the emulated TTPs ineffective. This could lead to a limited number of findings or detection of the Red Team in the early stages of a scenario. As such, a scenario X can be created using innovative TTPs, with a higher chance of uncovering new findings and improvement opportunities.

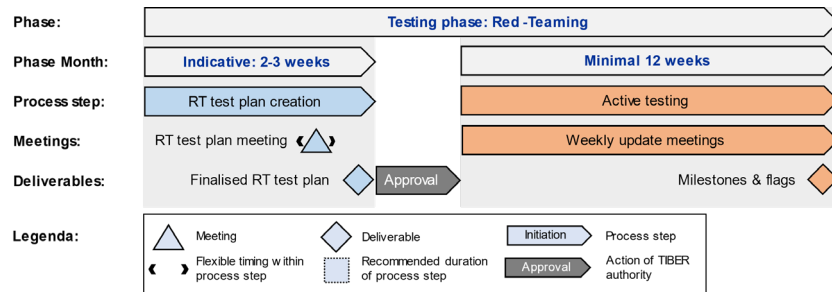
6.2.1.5. Step 4: Handover

At the end of the TI phase, once the TTI report is complete, a TI handover meeting will be organised by the CTL. During this meeting, the TI provider will present the TTI report to the Control Team, the TCT-FR and the Red Team allowing them to give feedback and to request some final adjustments to the report.

Once the TI provider has incorporated any feedback from the different participants and delivers the final TTI report, the engagement can officially move into the Red Teaming phase. To facilitate the accurate execution of the prescribed scenarios, the TI provider must remain available to advise the Red Team throughout the Red Teaming phase. Participation of the TI provider in the Red Teaming phase allows for further support in the event that the Red Team has specific questions about the Threat actor emulated during the RT activities.

6.2.2. The Red Teaming (RT) sub-phase

The TTI Report will be used by the RTT to develop attack scenarios and execute an intelligence-led red team test of specified critical live production systems, people and processes that underpin the entity's CFs.



Source: TIBER-EU.

Inputs of the phase	Outputs of the phase
Targeted Threat Intelligence report (TTIR)	Red Team Test Plan
TIBER-EU Guidance for the Red Team Test Plan	Red Team status updates
Red Team status update guidelines	Red Team Report (draft)
TIBER-EU Guidance for the Red Team Test Report	
TIBER-EU Purple-Teaming Best Practices (if needed)	

6.2.2.1. Red Team Test Plan

The RT is expected to formally document a detailed timeline for each scenario, including planned TTPs and a description of the required leg ups³ if these TTPs are to be unsuccessful. TIBER-FR requires each scenario to be split up into four distinct sub-phases: RECON,⁴ IN,⁵ THROUGH,⁶ OUT;⁷ to categorise the TTPs used by the RT in an effective manner. Furthermore, it is requested that the Red Team also maps all TTPs it will use to the MITRE ATT&CK framework to get a clear and standardised overview of the proposed attack plan. The plan will be shared with the CT and TCT-FR, allowing them to provide feedback to refine the plan where needed.

An important part of the RT test plan focuses on alternative approaches and required leg ups. The RT is expected to anticipate any issues during testing (detection, ineffective TTPs, etc.) by formulating alternatives to the chosen TTPs or potential leg ups that could be used to conduct further testing.

³ During the testing process, the RTT may be unable to progress to the next stage owing to time constraints or because the entity has been successful in protecting itself. In such scenarios, the RTT, with agreement from the CT and TM, may be given a "leg-up", whereby the entity essentially gives the RTT access to its system, internal network, etc. to continue with the test and focus on the next flag/target.

⁴ Reconnaissance.
⁵ Intrusion and persistence.
⁶ Lateralization.
⁷ Impact.

6.2.2.2. Test execution

- Execution of the scenarios

Once the Red Team test plan is approved by the CT and the TCT-FR, the execution of the scenarios can begin. In the RT test plan, the Red Team has detailed the specific TTPs that will be used as well as a timeline roughly setting out each scenario sub-phase (RECON-IN-THROUGH-OUT). However, a more pragmatic approach is required when executing the different scenarios, allowing for small deviations (meaning with no impact on the TIBER-FR engagement planning and/or the test risk assessment) from the test plan as the Red Team gains a better insight into the infrastructure and security controls in place.

The objective of the Red Team is to capture the flags related to each of the scenarios. Of course, the actions undertaken by the RT are intended to be shared with and approved by the CT, especially the actions related to capturing the flags. The execution of each scenario should be performed in a stealthy way so as to avoid detection by the Blue Team, consistent with the modus operandi of real threat actors.

When detection events do occur, the CT is encouraged to refer to TIBER-EU Purple Teaming Best Practices. This way, other testing activities can continue without the knowledge of the BT, maintaining the Red Teaming nature of these TTPs.

- Definition and role of the “Leg ups”

20

As stated above, the Red Team is subject to several limitations compared to the threat actors emulated when executing TIBER-FR RT scenarios. Due to these limitations, it is possible that the RT will face difficulties in successfully executing a scenario drafted by the TI provider. The TIBER-EU framework has taken this into account by enabling the activation of measures that would allow the RT to proceed with the scenario, known as “leg ups”.

A leg up can be defined as an action through which the CT assists the RT in executing the scenario and capturing the related flags. Leg ups serve to maximise the value of a TIBER-FR engagement as they allow the RT to continue executing the scenario, possibly enabling the identification of findings in the latter stages of the test. The leg up provided strongly depends on the scenario and the level of access available to the RT.

They can be categorised as follows (non-exhaustive list):

- **Time saving leg ups:** these leg ups are granted to accelerate the progress of the RT. The RT is not necessarily blocked but would require significant time to proceed with the scenario execution, however, given enough time, the RT would overcome the control (e.g. Identifying suitable target machines on an internal network the RT has access to).
- **Information leg ups:** these leg ups provide the RT with information on how to proceed with the scenario (e.g. Explaining why a payload used by the RT was blocked/detected, allowing the RT to make adaptations).
- **Access leg ups:** these are leg ups where the CT provides specific access to the internal network or infrastructure to perform an action that would help the RT (e.g. as an accomplice opening a phishing email). The CT can also provide access for the RT, granting them a foothold in the internal network (e.g. RT is provided with an account that has a specific access). This is always done on the assumption that, given enough time, the RT would reach this level of access.

Point of attention, leg ups must be obtained by the CT following usual processes and procedures of the tested entity and must be realistic (example not to follow: requesting a trainee account with inappropriate access that a trainee would never have).

The RT is expected to anticipate any leg ups they may require during the scenario execution, identifying them in the RT test plan. Having leg ups that are known in advance also enables the CT to adequately prepare for leg up activation. This minimises the risk of delays during testing, as the leg up can be prepared well before it is actually needed. Activation of a leg up should be carried out in consultation with the CT and pending non-objection by the TCT-FR.

- **Red Team status updates**

The Red Teaming phase is the most critical phase of a TIBER-FR engagement. Red Team testers are actively attacking the CI live production systems in their search for set flags and relevant findings. This activity inherently comes with risks for the CI's business operations, balanced by the risk mitigating actions taken in the preparation phase. **It is therefore essential that the CT and TCT-FR are aware of the actions planned and performed by the RT, ensuring the test can be conducted in a controlled manner.**

During the Red Team phase, **the CT will be in close contact with the Red Team testers. A short daily meeting or call should be arranged for this purpose.** On these daily update calls, the RT will inform the CT about any issues encountered as well as the activities planned for the next day. Additionally, a more continuous channel of communication could be set up, such as a secure instant messaging channel, to update the CT (and possibly the TCT-FR) on the RT activities the moment they occur.

Besides the CT, **the TCT-FR should also be updated on a regular basis** about the RT activities and any potential issues encountered. For this purpose, typically **a weekly update by the RT suffices unless the TCT-FR requests otherwise.** During this weekly call, the RT is expected to provide an overview of the activities performed over the past week, the findings so far, any issues or blocking factors, and the activities planned for the coming week along with an updated project plan. A template slide deck for this meeting is provided by the TCT-FR by means of guidance and the RT is free to decide how to present the information requested.

21

Participation of the TI provider is also encouraged for these weekly calls to support the Red Team and provide input. One specific example where TI input could be beneficial is during the reconnaissance activities performed by the RT. The passive nature of the reconnaissance activities performed in the TI phase might result in a gap between the information provided by the TI provider and the information the RT needs to properly execute the prescribed scenarios. For this reason, the RT often performs preliminary active reconnaissance to gain additional insights that could be useful for the scenario execution. Any findings made through the Red Team's active reconnaissance activities could be shared with the TI provider who can in turn give advice on how the emulated threat actor would make use of such findings, thus potentially influencing the planning or execution of the scenarios.

In case any critical issue is encountered during testing, an ad hoc meeting can be scheduled between the RT, CT and TCT-FR to discuss and look for possible solutions together.

- **Red Team Report**

When all testing activities have been concluded, the RTT drafts a Red Team report giving a detailed overview of the test.

The report contains the following aspects:

- An executive summary describing the test and the most important findings which should be concise and understandable at a strategic level (by the governing body);
- A detailed timeline describing all the RT actions and relevant information, including target systems and possible artifacts that remained on the CI network (this could be in a separate document);

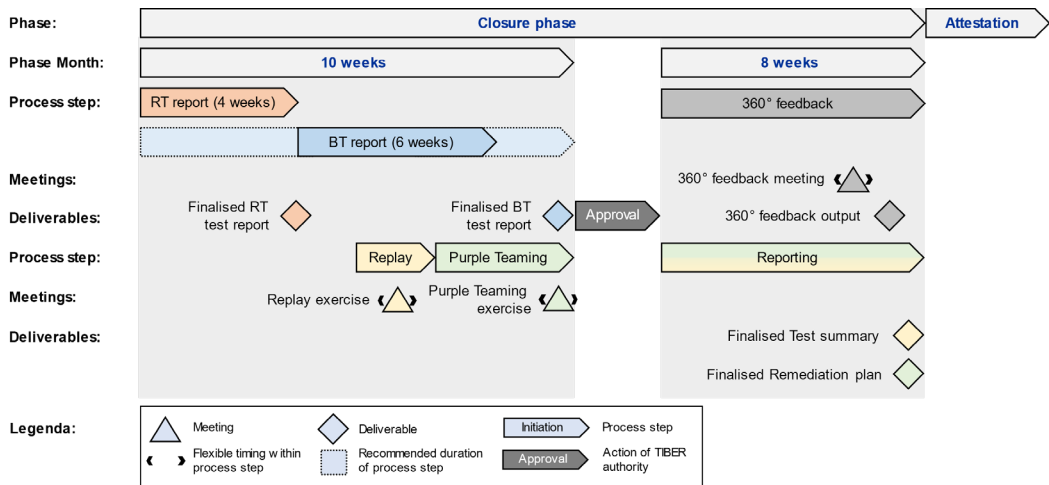
- Description of each of the scenarios detailing the TTPs used, any leg ups that were required and the results obtained;
- List of findings identified by the RT ranked according to severity, in the context of implemented security controls;
- Provider recommendations for each finding.

At the end of the RT phase, a draft version of this report is delivered to the CT. The final version of the report can be delivered during the engagement closure phase allowing for the inclusion of any additional findings from the replay and purple teaming activities.

6.3. The closure phase

When the Red Team phase is concluded, the TIBER-FR engagement moves into its closure phase.

During this phase, some workshops are held, and reports are drafted by the different test participants. The goal of the closure phase is to perform a return on experiment for the entire TIBER-FR engagement and its related findings, draft a remediation plan and provide feedback on the performance of all parties involved in the engagement.



Source: TIBER-EU.

Inputs of the phase	Outputs of the phase
Red Team report (draft)	Blue Team Report
TIBER-EU test summary report guidelines	Red Team Report (final)
TIBER-FR 360° feedback template	Test Summary Report (containing remediation plan)
TIBER-EU Purple-Teaming Best Practices	TIBER-FR attestation

6.3.1. Blue Team Report

Once the active RT phase is finished, the test can be disclosed to the BT. The BT is briefed on the scope of the assessment and provided with a high-level overview of the compromising actions performed by the RT. Using this information, the BT is expected to list any detection and response processes performed during the testing timeframe that could be linked to the RT testing activity. This information is then combined in a BT report that will serve as input for the next steps in the TIBER-FR closure phase.

6.3.2. Replay workshop and purple teaming exercise

In the replay workshop, the RT and BT come together to perform a walkthrough of the actions performed by both teams during the test. This workshop can therefore only be organised after the delivery of the BT report, as a detailed timeline from both the RT and BT is required for an in-depth discussion on the assessment. All participants need to be familiar with the RT Test Report and the BT Test Report prior to the Replay Workshop. The required participants for this workshop are the Red Team, the Blue Team, the Control Team and the TM. Participation of the TI provider in this workshop is not a requirement, but it is possible. If deemed useful by the CT, it is also possible to include the TI provider in this workshop to provide further insight into the scenarios developed.

Typically, the replay workshop is comprised of two main parts:

- **A “tabletop” walkthrough of the test is performed**, comparing the RT and BT timelines. The RT and BT explain their actions in further detail where required. The goal of this tabletop walkthrough is to identify areas where further investigation could be beneficial (e.g. RT actions that went undetected by the BT, or BT detections that could be avoided by making small adjustments to the RT approach).
- **The second part of the replay workshop is more hands-on**. Where possible, the RT re-enacts (part of) some of the attacks performed during the Red Teaming phase and the BT investigates whether they can detect these attacks and respond accordingly. This can be an iterative process, where slight modifications are made to both RT and BT actions, thus maximising the learning value for both parties.

The duration of the replay workshop can vary, but it is recommended to reserve at least two half-day sessions for it.

The replay workshop is further augmented with a purple teaming activity as outlined in the TIBER-EU purple teaming best practices.

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

- Relevant issues that could not be tested during the active testing phase particular vulnerabilities identified during the test.
- Other steps which could have been taken by the RT and potential BT responses.
- Alternative scenarios and their potential consequences.
- Proof of concepts.
- Discussion of anticipated remediation measures with the RTT.
- Business continuity exercises.

The PT exercise must take place within ten weeks after the end of the active testing, the participants are at least: the CT, BT, RT.

6.3.3. Test Summary Report

When both the Red Team and the Blue Team have finalised their reports, **the Control Team is expected to compile a Test Summary report**. This report combines the RT and BT views on the test and provides a high-level overview of the course of the TIBER-FR engagement.

Some elements of the test summary report can already be completed during the test preparation and execution phases. The CT is therefore encouraged to start drafting the test summary report early in the engagement, reducing the report effort required in the closure phase.

The test summary report aims to provide a complete overview of the TIBER-FR engagement and its outcomes. As such, the CT is expected to list all findings made during the test. However, given the sensitive nature of the information, it is advisable that only a high-level description of the findings is included in the test summary report. This report is shared with the C-level (CEO and governance bodies) to ensure endorsement at the highest level.

6.3.4. 360° Feedback Workshop

In the 360° feedback workshop, the CT, TCT-FR, TIP and the RTT come together to review the TIBER-FR engagement on a more methodological level, giving feedback on the TIBER-FR process, the national implementation guide, and on the performance of each participant involved in the engagement. As TIBER-FR national implementation is of an evolving nature, this type of feedback workshop is useful to improve the practices and the way in which providers, TCT-FR and CI approach TIBER-FR engagements. The TCT-FR will arrange and facilitate this workshop, moderating the discussion to allow every participant to share experiences and provide feedback.

In preparation for this workshop, the TCT will send out a 360° feedback questionnaire to each participant. The participants are expected to fill in this questionnaire and return it to the TCT-FR before the workshop. The TCT will use the answers provided as input to moderate this discussion, but the completed questionnaires will not be shared with the other participants. Any feedback to enhance the TIBER-EU framework and its guidance will be anonymised and communicated to the TIBER Knowledge Center (TKC).

6.3.5. TIBER-FR/DORA TLPT attestation

When all TIBER-FR requirements have been met (including mandatory requirements set out in Annex I of the [TIBER-EU framework document which are aligned with DORA TLPT requirements](#)) and the required reports have been delivered to the TCT-FR, a TIBER-FR/DORA attestation is provided to the tested entity. This attestation is a document signed by all participants in the engagement and declares that the assessment complies with all TIBER-FR requirements. Therefore, the TIBER-FR attestation document is proof to other authorities that the CI has successfully completed a TIBER-FR/DORA TLPT assessment and can serve as the basis for mutual recognition of the engagement.

At any time when performing a test, the TCT-FR may consider that it is not compliant with TIBER-FR requirements if the performance, quality or secrecy of the test is compromised, e.g. in the event that:

- the TIP and/or the RTT has shown that it does not or cannot comply with the requirements or standards set out in the TIBER-FR national implementation guide;
- the test has been compromised by the RTT, the TIP or the tested entity either fraudulently, intentionally or as a result of gross negligence.

The TCT-FR will take this decision in consultation with the CT of the tested entity, unless the circumstances do not, in the opinion of the TCT-FR, allow for this. The TCT-FR will communicate the reasons for its decision to the involved parties. When the test is not recognised as compliant, the TIBER-FR/DORA TLPT attestation is not delivered to the tested entity, and the test will not be taken into account for the 3-years cycle of TIBER-FR engagements. For a multi-jurisdiction Joint test, the decision is made in consultation with the other involved TCTs. The entity is allowed to continue the test for its own benefit even if it is not recognised as a TIBER-FR test.

Intellectual Property

Each participant will retain the intellectual property rights (“IP Rights”) already owned or developed prior to or in parallel with, but outside the scope of, each test. Each participant will retain ownership of all of its data, codes, information and elements of any kind transmitted in respect of each test and will return to the other participants all documents and files previously transferred for the purposes of the test that are considered to be the other participant’s IP Rights. The ownership and use of IP Rights developed jointly or individually, in the course of and within the scope of each test will be separately determined.

