EUROPEAN CENTRAL BANK
EUROSYSTEM

TIBER-EU White Team Guidance

The roles and responsibilities of the White Team in a Threat Intelligence-based Ethical Red Teaming test

December 2018

Contents

1 Executive Summary

The Threat Intelligence-based Ethical Red Teaming (TIBER-EU) Framework enables European and national authorities to work with financial infrastructures and institutions (hereinafter referred to collectively as “entities”[1]) to put in place a programme to test and improve their resilience against sophisticated cyber attacks.

The ECB published the TIBER-EU Framework (TIBER-EU Framework: How to Implement the European Framework for Threat Intelligence-based Ethical Red Teaming)[2] and TIBER-EU Services Procurement Guidelines[3], respectively. This TIBER-EU White Team Guidance (“Guidance”) is referred to in, and is an integral part of, the TIBER-EU Framework.

TIBER-EU is an instrument for red team testing, designed for use by core financial infrastructures, whether at national or at European level, which can also be used by any type or size of entity across the financial and other sectors. At the same time, TIBER-EU is designed to be adopted by the relevant authorities in any jurisdiction, on a voluntary basis and from a variety of perspectives, namely as a supervisory or oversight tool, for financial stability purposes, or as a catalyst.

TIBER-EU facilitates red team testing for entities which are active in more than one jurisdiction and fall within the regulatory remit of several authorities. TIBER-EU provides the elements allowing either collaborative cross-authority testing or mutual recognition by relevant authorities on the basis of different sets of requirements being met.

When an authority adopts TIBER-EU, tests will only be considered TIBER-EU tests when they are conducted in accordance with the TIBER-EU Framework, including the TIBER-EU Services Procurement Guidelines and the TIBER-EU White Team Guidance.

The team that manages the test, in accordance with the TIBER-EU Framework, within the entity that is being tested, is called the White Team. The purpose of this document is to provide further guidance about the roles and responsibilities of the White Team.

1.1 What is TIBER-EU?

TIBER-EU is a framework that delivers a controlled, bespoke, intelligence-led red team test of entities’ critical live production systems. Intelligence-led red team tests mimic the tactics, techniques and procedures of real-life threat actors who, on the

[1] For the purposes of the TIBER-EU Framework, “entities” means: payment systems, central securities depositories, central counterparty clearing houses, trade repositories, credit rating agencies, stock exchanges, securities settlement platforms, banks, payment institutions, insurance companies, asset management companies and any other service providers deemed critical for the functioning of the financial sector.

[2] TIBER-EU FRAMEWORK.

[3] TIBER-EU Services Procurement Guidelines.

basis of threat intelligence, are perceived as posing a genuine threat to those entities. An intelligence-led red team test involves the use of a variety of techniques to simulate an attack on an entity's critical functions and underlying systems (i.e. its people, processes and technologies). It helps an entity to assess its protection, detection and response capabilities.

1.2 What is the White Team?

The White Team is the team – within the entity being tested – that is responsible for the overall planning and management of the test, in accordance with the TIBER-EU Framework. The members of the White Team are the only people within the entity being tested that know that a TIBER-EU test is taking place. The White Team must ensure that the TIBER-EU test is conducted in a controlled manner, with appropriate risk management controls in place, while maximising the learning experience for the entity. For this the White Team must closely cooperate with the TIBER Cyber Team (TCT)[4] from the respective authority.

1.3 What is the TIBER-EU White Team Guidance?

The Guidance is divided into four parts:

- the roles and responsibilities of the White Team during the preparation, testing and closure phases of a TIBER-EU test;
- the composition of the White Team;
- the requisite skills and experience of the White Team;
- the organisational aspects of the White Team.

The White Team Guidance is an integral part of the TIBER-EU Framework. Further details on the TIBER-EU Framework can be found in the document "TIBER-EU Framework: How to implement the TIBER-EU Framework". Any further enquiries about TIBER-EU should be sent to TIBER-EU@ecb.europa.eu.

[4] The TCT is the team at the authority that: (i) facilitates the TIBER-EU tests across the sector; (ii) provides support and specialist knowledge to White Team Leads (WTLs, responsible for the entity's test management); (iii) acts as the contact point for all external enquiries; and (iv) supports the overseers and supervisors during and/or after the tests (if the overseers and supervisors are not included in the TCT). For a comprehensive description see the TIBER-EU Framework.

2 Introduction

2.1 Purpose of this document

The White Team is the team – within the entity that is being tested – that is responsible for the overall planning and management of the test, in accordance with the TIBER-EU Framework. This document provides information about its roles, responsibilities and other relevant organisational aspects.

2.2 Structure of the White Team Guidance

The White Team Guidance is structured as follows:

- Chapter 3 sets out the role and responsibilities of the White Team during the preparation, testing and closure phases of a TIBER-EU test;
- Chapter 4 provides guidance on the composition of the White Team and on the different types of profiles required within the entity and possibly from the entity's third-party providers;
- Chapter 5 provides guidance on the skills and experience needed for the different functions in the White Team to manage the test;
- Chapter 6 provides guidance on the organisation of the White Team during the TIBER-EU test.

2.3 Target audience of the White Team Guidance

This White Team Guidance is aimed at:

- authorities responsible for adopting, implementing and managing the TIBER-EU Framework at national and European levels;
- entities looking to undertake TIBER-EU tests;
- supervisors and overseers of those entities;
- third-party providers that may be included in the scope of the test of entities;
- organisations interested in providing cyber threat intelligence services under TIBER-EU (threat intelligence (TI) providers);
- organisations interested in providing red team testing services under TIBER-EU (red team (RT) providers).

Although the TIBER-EU Framework is aimed at the financial sector, it can be applied by other sectors and industries for testing other types of entities.

3 Roles and Responsibilities of the White Team

This chapter describes the roles and responsibilities of the White Team and how these interact with the other involved parties. For more clarity on the roles and responsibilities of the different stakeholders involved in the overall process of a TIBER-EU test, a Responsibility Assignment (RACI) Matrix is included in Annex I.

3.1 Roles of the White Team

The end-to-end conduct of a TIBER-EU test is the responsibility of the entity being tested.

For each TIBER-EU test, there should be a White Team belonging to the entity, with a dedicated White Team Lead who is responsible for coordinating all TIBER-EU test-related activities including:

- the overall planning;
- engagement with threat intelligence/red team[5] (TI/RT) providers;
- management of the separate phases of the test:
  - the preparation phase (which includes scoping and procurement);
  - the testing phase;
  - the closure phase;
- coordination with other stakeholders, including meetings with the TCT and authorities.

3.2 Responsibilities of the White Team

The White Team will be responsible for the end-to-end conduct of a TIBER-EU test and for managing the separate TIBER phases, to ensure the TIBER-EU test is conducted in a safe and controlled manner. The White Team is responsible for leading the preparation phase, overseeing the testing phase (which includes gathering threat intelligence and red teaming) in close collaboration with the TI and RT providers, and leading the closure phase. The White Team fulfils its duties in close collaboration with the TCT and its responsible TIBER Test Manager (TTM), who are not part of the

[5] TI providers deliver a detailed view of the specific entity's attack surface and help to produce actionable and realistic testing scenarios. The RT provider plans and executes a TIBER-EU test of the target systems and services, which are agreed in the scope.

entity’s White Team. The TTM is a representative of the authority and should be in direct contact with the White Team throughout the entire test.

The main responsibilities of the White Team are set out below.

- Ensure that all the risk management controls are in place and effective, to ensure that the test is conducted in a controlled manner, and that any business impact from the test is within the risk appetite of the entity.
- Involve all relevant stakeholders during the preparation phase and ensure that the critical functions are included within the scope to facilitate a realistic simulation of an actual advanced targeted attack.
- Procure the TI/RT providers in accordance with the TIBER-EU Services Procurement Guidelines.
- Liaise closely with the procured TI/RT providers and the TCT throughout the lifecycle of the TIBER-EU test.
- Ensure that all correct information flows and protocols are in place, so that the White Team is informed of all actions taken by the RT provider and is able to actively manage any risks.
- Ensure that the test is executed in a timely manner and within the defined scope, and provide guidance if the RT provider is deviating from the agreed scope.
- Manage all possible escalations arising because of the test, for example if an event arises as part of the actions of the RT provider. For this the White Team has to ensure that sufficient arrangements in place for it to be informed of actions taken by the Blue Team, by the target entity’s security or by the response capability, especially as White Team members are not formally part of the Blue Team.
- Make appropriate decisions if unforeseen circumstances arise during the test.
- Maximise the Blue Team’s learning experience.
- Consult with the entity’s board, to ensure that the scope and attestation are signed off in relation to the TIBER-EU test.

4 White Team composition

This chapter describes the types of staff profile that can make up the White Team. The size of the White Team will depend on the size of the entity, its organisational structure and its business model (e.g. use of third-party providers). Therefore there is no one-size-fits-all model for a White Team and its composition is likely to vary from entity to entity.

4.1 General considerations

The guiding principle should be that the White Team is as small as possible, but consists of the right people necessary to manage the test from inside the entity. This implies that the team's members need to strike a balance between: (i) the requisite skills (as detailed in Chapter 5) to manage an end-to-end test; (ii) sufficient business and operational knowledge of the entity and its critical functions, systems and processes; and (iii) the right level of authority to make critical decisions during the test, if required.

The White Team may therefore be composed of personnel belonging to the entity itself, to other group entities or to third-party providers.

The various compositions that a White Team may take must not, however, alter its responsibilities as per Section 3.2.

In any case, the authorities as stated in 4.7 must signal that they have no objection to the suggested composition.

Third-party provider(s)

If the entity being tested outsources part of its critical functions or other parts of the potential scope of the test to one or multiple third-party providers, the third-party provider(s) should be included in the scope of the test. The White Team Lead is advised to arrange a discussion with a trusted contact from the third-party provider(s) at an early stage, following a discussion with the TCT at the pre-launch meeting, to indicate the entity's intention to conduct a TIBER-EU test. The discussion with the third-party provider should be confidential. This is to ensure the integrity of the test, given that personnel from the third-party provider(s) will be part of the Blue Team. The same confidentiality conditions apply to both the third-party provider(s) and the entity itself.

A small number of staff from the third-party provider(s) can join the White Team, depending on the scope of the test. These staff should have detailed knowledge about the systems that the entity uses at the third-party provider(s).

One staff member from the third-party provider(s) should be the primary point of contact for the White Team Lead. This primary point of contact can join the relevant meetings as long as the scope of the test includes functions and systems of the third-party provider(s).

The entity being tested remains responsible and accountable for the overall test.

Multiple jurisdictions

When a group entity or pan-European entity with a presence in multiple jurisdictions is tested under TIBER-EU, the White Team should be established by looking at: (i) the scope of the test, (ii) where operations are run, and (iii) where relevant people and processes are active. Based on these considerations, the White Team Lead from the entity should determine the most appropriate composition of the White Team, making sure it has the most relevant people to ensure a safe and controlled test is conducted. Overall accountability lies with the White Team Lead from the jurisdiction where the lead authority is located. For information on the leading authority see the TIBER-EU Framework document.

4.2 White Team members

The following functions or types of personnel should be part of the White Team:

- a White Team Lead;
- subject matter experts;
- COO (or other C-level members with responsibilities in this area, like the CIO or CTO);
- CISO (or equivalent)[6];
- third-party provider(s) where applicable.

To protect the confidentiality of the test, the White Team should consist of no more than the five functions or types of personnel mentioned above. In smaller organisations it is possible for the White Team to consist of fewer functions. Each function is detailed below.

4.3 White Team Lead

The White Team Lead is the person who establishes the White Team, has the overall responsibility for the test and is the primary point of contact for the TCT.

[6] Neither the COO nor the CISO will be involved in the day-to-day operations of the test.

Due to the importance of this role, it is important that at least one other member of the White Team is kept well informed about the test details so as to deputise for the White Team Lead if and when needed.

In some circumstances it can be beneficial or necessary to recruit an external White Team Lead. As entities differ in size and complexity and have different organisational structures and set-ups, the entity may opt to outsource the function of the White Team Lead to an external specialist with the right profile. For example, some entities may not have the right internal profile for a White Team Lead or if such a profile exists, the staff member may not be available for the entire lifecycle of the test due to other responsibilities.

4.4 Subject matter experts

Subject matter experts should have a broad range of specific knowledge, expertise and experience pertaining to the entity and its operations. This will enable them to provide the requisite information and insight during the test, which will allow the White Team Lead to make the appropriate risk-based decisions. The number of subject matter experts that make up the White Team will vary from entity to entity, depending on the entity’s size and complexity. Subject matter experts with the broadest range of skills and knowledge should be chosen so as to limit the number of them involved in the White Team.

4.5 C-level member

The COO (or other C-level member with responsibilities in this area such as the CIO or CTO) and/or the CISO (or equivalent) are the most senior individuals in the White Team, and act as the escalation point during the test. During the test, there may be moments when key decisions need to be made on how to progress from a risk perspective, and such decisions can only be taken by entity staff members with sufficient seniority. Although the C-level member is unlikely to be the White Team Lead or have an active and resource-intensive role during the test, their presence in the White Team will allow the White Team Lead to escalate matters to the decision-makers in full confidentiality. Furthermore, the C-level member who is member of the entity’s board will be responsible for agreeing the scope and signing the attestation on behalf of the entity.

In any multi-jurisdictional test of group entities, the C-level member should come from the overarching group where the entity is located or headquartered. In the case of a test which involves a third-party provider, there should be C-level membership in the White Team from both the entity and the third-party provider, and the scope of the test should be signed off at board level on both sides.

4.6 Other needed expertise

During different phases of the test, specific subject matter expertise may be needed (such as procurement or legal expertise). While these subject matter experts will not be day-to-day members of the White Team, they should be informed about the high-level aspects of the TIBER-EU test process and the need for secrecy. Experts used on an ad hoc basis during the test may also sign non-disclosure agreements (NDAs) to ensure the confidentiality of the test is maintained.

4.7 Discussion with the TIBER Cyber Team on the composition of the White Team

The TCT is not part of the White Team but works closely with the White Team during the test.

At the start of the process, the entity selects a White Team Lead based on the criteria set out in Section 5.1. It is then up to the White Team Lead to select subject matter experts for the White Team. The composition of the White Team is in principle up to the entity, but this has to be discussed with the TCT and the TCT must signal that it has no objection or further changes to the final composition of the White Team. If there are concerns that the criteria have not been met, the TCT has the authority to prevent the suggested composition of the White Team and/or invalidate a test for TIBER-EU recognition.

Within the EU, entities may operate their business across borders, with a presence in multiple jurisdictions. In such cases, the lead authority has to ensure that the composition of the White Team is in accordance with the criteria in Section 5.1 and that expertise from the different jurisdictions is properly reflected in the White Team composition. In cases of tests where multiple authorities are involved, the lead authority should reach out to the other relevant authorities to discuss the proposed composition of the White Team, giving them the opportunity to signal any objections.

5 Skills and experience

Due to the critical role of the White Team during a TIBER-EU test, its members should be selected based on specific skills and experience. This chapter outlines the skills and experience required for the specific functions of the White Team.

5.1 White Team Lead

One of the entity's members must be the White Team Lead. This person has overall responsibility for the test and is the primary point of contact for the TCT.

5.1.1 Skills

As the manager of the White Team and the TIBER-EU test, the following skills are essential for the White Team Lead:

- people and process management skills;
- ability to communicate with different levels of staff, from C-level to operational teams;
- ability to work under pressure;
- strong communication skills;
- ability to be pragmatic and decisive;
- strong project management skills.

5.1.2 Experience

In addition to the skills above, there are many areas in which the White Team Lead needs experience and knowledge. If the White Team Lead does not have some of these attributes, these would have to be supplemented by other members in the White Team.

The White Team Lead should as far as possible have the following experience:

- insight into and deep understanding of the entity and its infrastructure (including its IT landscape and business operations);
- experience working with other relevant departments of the entity (e.g. legal, procurement, communications, IT, business, security, fraud, etc.);
- experience in leading cyber resilience testing, specifically red team testing;

- experience with crisis management;

- experience with procurement processes, including knowledge of the relevant vendor market;

- general knowledge of privacy and security, and specifically their legal aspects, including the ability to identify when to involve the legal department.

5.2 External White Team Lead

If the entity outsources the role of the White Team Lead to an external person, it should ensure that the external White Team Lead possesses all the requisite skills and experience cited above. If the external White Team Lead does not possess all the necessary skills and experience, these must be supplemented by the other members in the White Team.

Given the intrusive and confidential nature of the test, the entity should take all the normal precautions like vetting and having the external White Team Lead sign an NDA, and should ensure that no sensitive data are kept by this person or the company from which the White Team Lead is hired. If the external White Team Lead is from a specialist external provider, the entity should carry out the required due diligence on this person and/or the company the White Team Lead is hired from, ensuring that they have the right skills, expertise, qualifications, experience and security measures in place to manage a TIBER-EU test.

Any such arrangements should be formalised through contracts. Further guidance on the principles for such procurement can be found in the TIBER-EU Services Procurement Guidelines. This is important, as the role of the White Team Lead is critical for such a sensitive test, and therefore the specialist external provider should be able to demonstrate its expertise in providing staff that can deliver such services.

To avoid any conflict of interest, the external White Team Lead cannot also work at the same time for the TI or RT provider procured for the TIBER-EU.

5.3 Skills and experience of the White Team members

The other White Team members, or more specifically the subject matter experts, should also have certain skills and experience to make sure they are able to fulfil the tasks of the White Team. The COO and CISO are functions predefined by the entity itself; as such no specific skills and experience have to be set for those functions.

The specific skills and experience that should be met collectively, as far as possible, by the subject matter experts in the White Team are as follows:

- extensive and specific knowledge of business processes within an entity;

- extensive knowledge of the IT landscape of the entity;

- sufficient risk management knowledge;
- sufficient experience in project management;
- experience in cyber resilience testing, including red team testing;
- sufficient up-to-date knowledge of tactics, techniques and procedures used by cyber threat actors.

Not every subject matter expert needs to possess all of the above-mentioned skills and experience, but all skills and experience should be met by them as a whole.

6 Organisation

There are a number of organisational considerations that the White Team must take into account when conducting a TIBER-EU test. These are outlined below.

6.1 White Team governance

The TIBER-EU test is performed under the responsibility of the tested entity itself. The board of the entity should delegate responsibility for managing the TIBER-EU test to the White Team Lead, who is responsible for the day-to-day management of the test and the decisions and actions taken by the White Team.

The White Team has to operate separately and independently from both the Red Team and the Blue Team, especially during the testing phase, to protect the secrecy and integrity of the TIBER-EU test.

The White Team members are the only people within the entity being tested that know that a TIBER-EU test is taking place. Therefore it is integral that the identity of the White Team is kept secret.

Due to the importance of the White Team Lead, it is important that at least one other member of the White Team is kept well informed about the test details, so as to deputise for the White Team Lead when needed. Above all, the White Team members should not disclose any information about the test beyond the White Team, and may sign an NDA to ensure the confidentiality of the test is maintained. For more on confidentiality and NDAs see Section 6.7.

Due to its responsibilities, the White Team Lead can make decisions that have a significant impact on the test and potentially on the continuity of the critical functions of the entity. Therefore the entity must ensure that the governance arrangements around the White Team are well considered and robust.

If circumstances require, the White Team Lead can consult the entity’s senior management (e.g. COO or CISO) to address any issues regarding the business continuity of the entity or the continuity of the test. However, any such consultation must be conducted via secure communication channels to ensure the conduct of the test remains secret and confidential.

6.1.1 Authority

In order for the White Team Lead to fulfil its responsibilities during a TIBER-EU test, no matter if this person is internal or external, he or she needs to be given:

- authority and mandate within the entity to take full control of the testing process;

- direct access to senior management.

6.2 Time resources

During all the TIBER-EU test phases, the White Team members have to be able to dedicate enough time to their respective roles.

The table below gives an indication of how much time is likely to be spent by the White Team Lead and the other members of the White Team during the different phases of the TIBER-EU test. This is just an indication and the amount of time spent will differ per test based, for example, on the size of the entity, the scope, the longevity of the red team test and the experience of the different people involved.

Table 1
Time resources indication White Team

Test phase	Hours spent by White Team Lead	Hours spent by each remaining member of the White Team
Preparation phase **4-6 weeks excluding procurement**	8-16 hours per week	4-8 hours per week
Test phase TI **5 weeks**	8-16 hours per week	4-8 hours per week
Test phase RT **12 weeks**	10-30 hours per week	8-16 hours per week
Closure phase **4 weeks**	8-16 hours per week	4-8 hours per week

6.3 Responsibilities of the TIBER Cyber Team

The TTM is independent of the White Team and is part of the authority's TCT. The TTM's role is to oversee the conduct of the end-to-end test at the respective authority and ensure that it is being conducted in line with the TIBER-EU Framework. In cases where the TIBER-EU test has not been conducted in line with the TIBER-EU Framework, the TTM and TCT can invalidate the test and not recognise it as a TIBER-EU test.

As the TTM is the main contact for the White Team, he/she should be consulted on all issues throughout the test. In order to facilitate an open and successful test, it is critical that the White Team and TCT take a collaborative approach. Both parties should work together to foster a spirit of trust and cooperation, and there should be clear communication channels between them. The TCT and the White Team should regularly use the meetings that are part of the TIBER-EU process as a way to discuss whether the test is still proceeding as per the TIBER-EU Framework's specifications and to ensure that the learning experience of the entity is maximised.

6.4 Contact with the threat intelligence provider

The White Team Lead is responsible for liaising with the TI provider in order to ensure that the output of the threat intelligence phase is accurate, up to date and usable for the next phase of the TIBER-EU test.

6.5 Contact with the red team provider

The RT provider should keep the White Team, or at least the White Team Lead, constantly informed about ongoing actions so that the White Team has a clear picture throughout of the status of the test. The White Team and the RT provider should agree that the latter will always provide notice before executing any action affecting the entity. In this way the White Team can always differentiate an unrelated attack from an action based on the TIBER-EU test.

During the red teaming phase of the test, contact with the RT provider may take place daily or even multiple times each day. Any interaction between the White Team and RT provider should be conducted using safe and secure channels. It is highly recommended that important meetings such as the launch and scoping meetings are held as physical meetings to improve relationships between the relevant stakeholders and to foster a common understanding. During the testing phase the weekly test update meetings should also be held in person wherever possible.

6.6 Managing escalations

If actions taken by the RT provider are detected during the red teaming phase, it is likely that the Blue Team will escalate this, considering it to be a real-life cyber attack.

Escalation is a key part of the test, as the TIBER-EU test also aims to evaluate the entity’s detection and response capabilities. However, just like all other parts of the test, it needs to be controlled. For this reason, it is important for the White Team to manage all possible escalation paths within the entity. The White Team should only intervene and stop an escalation if it will have an unwanted business or critical impact or will involve external parties where this is not desired. For example, if critical servers are shut down by the Blue Team to stop the attack or a police report is filed, the White Team Lead should intervene and pause the test in order to deal with the escalation, while giving as little information as possible in order for the test to continue. In such cases the White Team’s intervention to stop escalation goes via the CISO or COO, depending on the arrangements agreed upon beforehand.

6.7 Confidentiality and non-disclosure agreement

To maximise the learning experience of the TIBER-EU test, no one outside of the White Team should be informed about the test. If the Blue Team is informed about the TIBER-EU test, the integrity of the test will be compromised and the entity will not learn about its capacity to detect and respond to unexpected cyber attacks. If the entity and/or the White Team inappropriately discloses details of the test to the Blue Team, the TCT has the authority to invalidate the test and not consider it as a TIBER-EU test.

However, conducting such intrusive tests secretly without the knowledge of people outside the White Team and TCT can be difficult. Furthermore, it may prove problematic for the White Team members to conduct their daily responsibilities without raising suspicion. In such cases, as a form of protection for the White Team members and to ensure that confidentiality is kept, the White Team members should sign a confidentiality or non-disclosure agreement at the inception of the TIBER-EU test.

7 Annex

RACI Matrix for a TIBER-EU test[7]

Requirement	Responsible	Accountable	Consulted	Informed	Documents
Adoption and Implementation					
The TIBER-EU Framework is adopted and implemented	Authorities	Authorities	Financial and cyber security sector	Financial and cyber security sector	Notice to TIBER-EU Knowledge Centre and TIBER-XX Guide
Preparation Phase					
Pre-launch meeting	TTM	TTM	WT	n/a	TIBER-XX Guide, TIBER-EU Services Procurement Guidelines, TIBER-EU White Team Guidance
Launch meeting	WT	Board of financial institution	TTM	n/a	n/a
Procurement process and formal contracts between the different stakeholders	WT	Board of financial institution	TTM	TI/RT providers	TIBER-EU Services Procurement Guidelines, contracts
Pre-test risk assessment	WT	Board of financial institution	TTM	TI/RT providers	Risk assessment
Scoping meeting	WT	Board of financial institution	TTM	TI/RT providers, if available	TIBER-EU Scope Specification document
Testing phase: threat intelligence					
Produce a generic threat landscape (GTL) report for financial sector	Authorities and/or sector and/or TI providers	Authorities and/or sector and/or TI providers	Possibly national intelligence agency/national cyber security centre/high-tech crime unit	Authorities and/or sector	GTL Report
Produce a dedicated TTI report on the financial institution, setting out threat scenarios which can be used by the RT provider	TI provider	WT	TTM, RT provider, possibly national intelligence agency/national cyber security centre/high-tech crime unit	n/a	TTI report
Testing phase: RT test					
Handover session between TI and RT providers, providing the basis of the threat scenarios	TI provider	WT	RT provider, TTM	n/a	TTI report
Scenario development for TIBER-EU RT test	RT provider	WT	WT, TTM, TI provider	n/a	RT test plan
Weekly test meetings or updates	WT	Board of the financial institution	RT provider, TTM	n/a	n/a
Discussion as flags are captured or when leg-ups are required	RT provider	WT	TTM	n/a	n/a
Closure phase					
RT test report, outlining the findings from the test	RT provider	WT	Senior executive responsible for cyber resilience at financial institution	TTM	RT test report
Blue Team report, which maps the Blue Team's actions alongside the RT	BT	WT	RT provider	TTM	Blue Team report

[7] Please refer to Section 11.2 (Table 5) in TIBER-EU FRAMEWORK.

provider's team actions					
Conduct an interactive replay of the test	WT	Board of financial institution	RT providers, TI provider, BT	TTM	n/a
360-degree feedback meeting	TTM	TTM	WT, BT, TI/RT providers	n/a	360-degree feedback report
Remediation plan to address the findings	WT	Board of financial institution	TI/RT providers, TTM	Supervisor and/or overseer, if not involved during the test	Remediation plan
Produce test summary report	WT	Board of financial institution	TI/RT providers, TTM	Other relevant authorities	Test summary report
Signed attestation to validate the true and fair conduct of the TIBER-EU test	Board of financial institution	Board of financial institution	WT, TI/RT providers, TTM	TTM and other relevant authorities	Attestation

Source: ECB

Abbreviations

BT	Blue Team
GTL	Generic threat landscape
NDA	Non-disclosure agreement
RACI	Responsibility Assignment Matrix (RACI stands for Responsible, Accountable, Consulted, Informed)
RT provider	Red team provider
TCT	TIBER Cyber Team
TIBER	Threat intelligence-based ethical red teaming
TI provider	Threat intelligence provider
TTI	Targeted threat intelligence
TTM	TIBER Cyber Team Test Manager
WT	White Team

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

For specific terminology please refer to the ECB glossary.