CONSOB | Commissione Nazionale per le Società e la Borsa
Autorità italiana per la vigilanza dei mercati finanziari

BANCA D'ITALIA
EUROSISTEMA

IVASS
Istituto per la Vigilanza sulle Assicurazioni

TIBER-IT
National Guidance

Threat Intelligence Based Ethical Red-Teaming – Italy

August 2022 - version 1.0

Francesco Trombadori, *Mattino a Ponte Fabricio*, the Bank of Italy's collection

Designed and printed by the Printing and Publishing Division of the Bank of Italy

INDEX

1 Introduction

1.1 Foreword

In recent years, cyber resilience has become an international priority due to the increasing sophistication and persistence of cyber risks because of the growing digitalisation and interconnectedness of financial services.

To address the growing cyber risks, the financial authorities have taken significant steps towards strengthening the cyber resilience of financial entities and the sector as a whole.

In 2016, the G-7 published the 'Fundamental elements for cyber security in the financial sector (G7FE)', while the CPMI-IOSCO published the 'Guidance of Cyber Resilience for Financial Market Infrastructures', which recognise testing, including red teaming exercises, as a key overarching component for an effective cyber resilience posture. Moreover, the G7 'Fundamental Elements for Threat-Led Penetration Testing (G7FE-TLPT)' document, published in 2018, provides guidance for entities to assess their resilience to malicious cyber incidents through simulation and for the authorities to consider the use of Threat-Led Penetration Testing (TLPT) within their jurisdictions. In the same year, the ECB published the TIBER-EU framework.[1]

At national level and in accordance with their respective powers, the Bank of Italy, the National Commission for Stock Exchange and Markets (Consob) and the Institute for the Supervision of Insurance (IVASS) cooperate to enhance the overall resilience of the Italian financial system. This collaboration is shaped by international and European frameworks and is conducted through supervisory activities, continuous regulatory-industry dialogue and intense public-private cooperation, rooted in dedicated national cooperative bodies.[2]

In early 2020, the Bank of Italy and Consob launched a joint action plan to enhance the cyber resilience of the Italian financial sector, by applying specific measures addressed to payment systems, central counterparties, central securities depositories and trading venues. The plan envisages the adoption of tools already developed by the Eurosystem, including, among other things, the Cyber Resilience Oversight Expectations (CROE) and TIBER-IT, i.e. the national implementation of the TIBER-EU framework. The banking and insurance subsectors are also expressing growing interest in the execution of TLPT, as an effective practice to enhance the cyber resilience of intermediaries. Banking and insurance regulators and supervisors are therefore engaged in the adoption and implementation of the TIBER-IT.

In order to implement the TIBER-EU framework, TIBER-IT provides a methodology and an operational model that can be adopted by financial entities and insurance undertakings on a voluntary basis to test and improve their own protection, detection and response capabilities.

---

1 https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf

2 The Italian Financial CERT (CERTFin) and Financial Unit for Business Continuity (Codise).

Throughout the process, the TIBER-IT tests involve strong multi-stakeholder engagement. Prior to the formal start of a test, entities appropriately identify and engage with key stakeholders, including the relevant authorities.

In accordance with the TIBER-EU framework multi-stakeholder engagement aims to support crossborder TIBER-IT tests, in particular for entities involved in cross-jurisdictional assessments, to promote fair discussions with respect to the mutual acceptance of TIBER-IT results and to improve protocols for the sharing of deliverables from the TIBER tests, also leveraging the TIBER-EU Knowledge Centre (TKC) set up at the ECB.[3]

Since TIBER-IT tests are highly sensitive and intrusive by design, when conducting these tests, all relevant stakeholders, and particularly the White Team (WT, see §3.2.3), should give high priority to clearly defining the scope of the test and applying effective risk management controls throughout the entirety of the assessment.

By performing TIBER-IT tests, financial entities improve their operational resilience considerably; financial authorities obtain adequate assurance with regard to their cyber resilience posture both at single entity and sectoral level, and national or European level, for financial stability purposes, where the framework is adopted by the major financial entities.

Against this background, the Bank of Italy, consistent with its mandate to safeguard monetary and financial stability, is the lead authority for TIBER-IT (the TIBER-IT Lead Authority), in close collaboration with Consob and IVASS in accordance with their respective powers. The maintenance of TIBER-IT and its alignment with TIBER-EU and other relevant international best practices are steered by a TIBER-IT cross-authority Steering Committee (TIBER-IT SC, see §3.2.1).

Throughout the rest of the document:

- the term 'Authorities' refers to the Bank of Italy, Consob and IVASS;
- the term 'financial entities', if not otherwise specified, includes financial market infrastructures, payment systems and supporting technological or network infrastructures,[4] trading venues, banks, payment and electronic money institutions, financial intermediaries,[5] insurance undertakings and intermediaries;[6]
- the term 'financial sector' includes the financial entities described above.

---

3 The TKC is a forum composed of representatives of the national authorities (e.g. NCBs) that have implemented the TIBER-EU framework in their respective jurisdictions. The TKC's key objectives are: i) maintaining the TIBER-EU framework; ii) facilitating the transfer of knowledge and promoting collaboration among jurisdictions; iii) supporting the national authorities in their national implementations and providing a centralised document repository; and iv) monitoring the national implementations in order to ensure the mutual recognition of TIBER tests.

4 'supporting technological or network infrastructure' means all the systems and implementations in support of one or more services instrumental for the payment ecosystem, for example: a) messaging and network services; and b) business services and/or applications for processing and exchanging financial and information flows, clearing and/or settlement of payment transactions (see the Regulation of 9 November 2021 issued by the Bank of Italy).

5 Pursuant to Article 106 of Legislative Decree 385/1993 (the Consolidated Law on Banking – TUB).

6 The latter where relevant for insurance distribution at national level.

1.2 What TIBER-IT is

The TIBER-EU framework requires national implementation in order to take into account national specificities and to ensure a cross-jurisdictional recognition of the tests. The Authorities carry out the national implementation of the TIBER-EU framework as described in this guidance. The Bank of Italy, in close collaboration with Consob and IVASS, leads and is responsible for the implementation and the maintenance of TIBER-IT.

TIBER-IT represents the national contextualisation of the TIBER-EU; its compatibility with other national TLPT frameworks and methodologies will be ensured to the greatest extent possible.

TIBER-IT mimics potential real attacks by reproducing the tactics, techniques and procedures (TTPs) of real threat actors, thus checking the detection, protection and response capabilities of the tested entity.

TIBER-IT is a voluntary guide, adopted to foster financial stability and cyber resilience, and adhering to it is not a regulatory, oversight or supervisory requirement.

1.3 Legal aspects

The transposition of the TIBER-EU framework and its contextualisation in the TIBER-IT National Guidance pivot mainly on the competencies attributed to the Bank of Italy, Consob and IVASS, on the overall stability, efficiency and competitiveness of the financial system,[7] as well as on those concerning the supervision of the regular functioning, reliability and efficiency of the payment system.[8] Indeed, such systems, strongly digitalised and interconnected, are susceptible to threats as a result of the increased sophistication and persistence of cyber risks.

In addition, similarly to what has been achieved in other jurisdictions, the adoption of the national framework is based on collaboration among the Italian financial system authorities, which includes Consob and IVASS, in pursuing the common interest of maintaining the overall resilience of the Italian banking, financial and insurance system. The TIBER-IT methodology and its voluntary adoption by financial entities aims at contributing to the enhancement of the cyber resilience of the system as a whole.

1.4 Purpose and scope of the Guidance

This guidance aims to improve the resilience of financial entities and the Italian financial sector as a whole, by providing a common approach for ensuring that the critical functions[9] (CFs) of financial entities are truly protected against targeted cyber-attacks.

---

7 Under Article 5, paragraph 1 of Legislative Decree 385/1993 (the Consolidated Law on Banking – TUB), Article 5, paragraph 1.c of Legislative Decree 58/1998 (the Consolidated Law on Finance – TUF) and Article 3, paragraph 1 of Legislative Decree No. 209/2005 (the Code of Private Insurance – CAP).

8 Under Article 146, paragraph 1 of the TUB.

9 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".

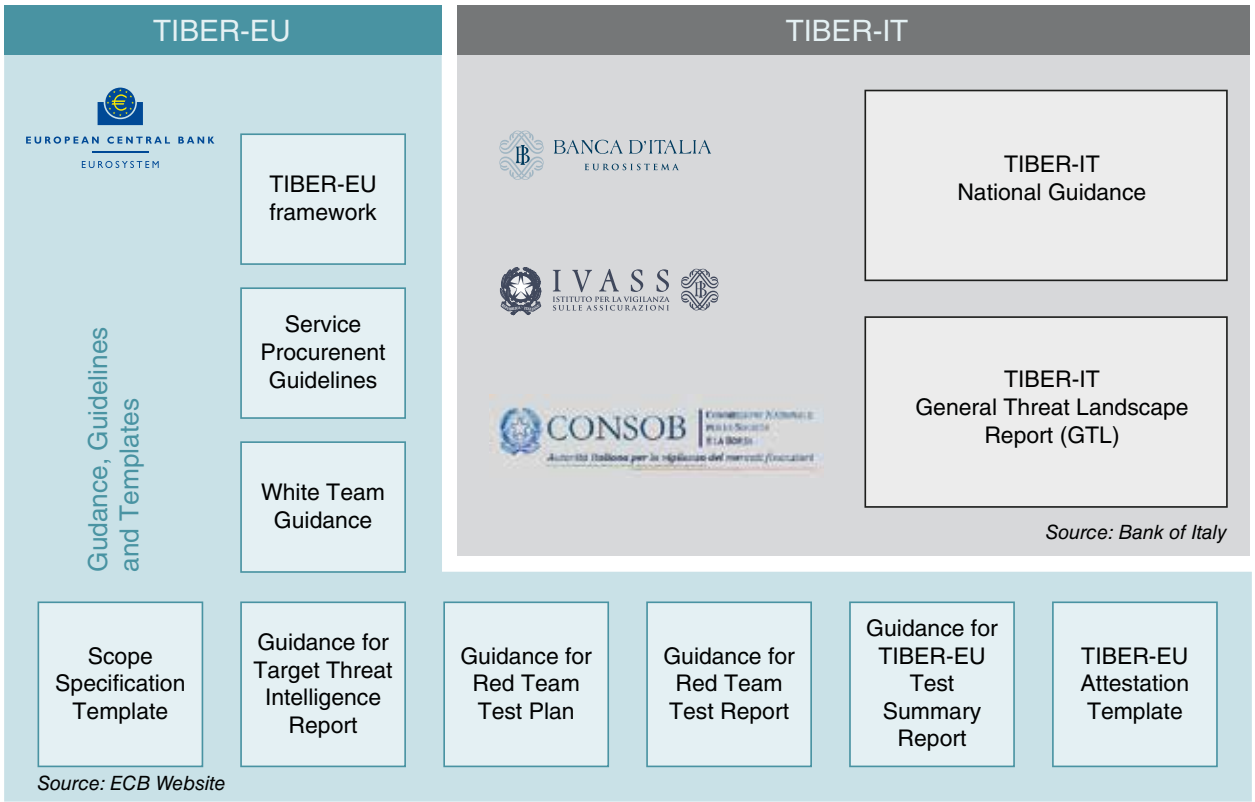
It provides an overview of how TIBER-EU is implemented in Italy. It explains the overall process and its key components such as its phases, activities, deliverables, roles and responsibilities as well as interactions among the different actors involved in a TIBER-IT test.

Financial entities allocate resources to plan and organise these tests on a voluntary basis according to this national guidance. The Authorities provide financial entities with methodological support and, when available, updated Generic Threat Landscape (GTL)[10] reports on the financial sector.

This national guidance is addressed to financial entities and their threat intelligence and red teaming service providers.

TIBER-IT should be read in conjunction with the TIBER-EU framework and its supplementary guidance. In particular, TIBER-IT refers to the documentation issued by the ECB, which is responsible for maintaining the framework at European level (Figure 1).

Figure 1: TIBER-IT OVERVIEW – KEY DOCUMENTATION AND INTERACTIONS WITH TIBER-EU



10 A GTL is a document describing the general threat scenario applicable to the financial system.

1.5 LEGAL DISCLAIMER AND COPYRIGHT NOTICE

The information and opinions expressed in this implementation guidance are for informational purposes only and are not intended to constitute legal or other professional advice.

Each entity that participates in a TIBER-IT test is solely and exclusively responsible and liable for the execution of the tasks attributed to it by this guidance, including compliance with the applicable laws and regulations.

Financial entities remain at all times fully responsible for the risk associated with the test and for any negative impacts on their services and on third parties.

This implementation guide is derived directly from the TIBER-EU framework, to which the ECB holds all copyright, and it is broadly aligned with TIBER-XX guides published in other EU countries, such as TIBER-NL, TIBER-DE, TIBER-DK, TIBER-BE, TIBER-IE and TIBER-FI and, as far as possible, with similar implementations in non-EU jurisdictions such as CBEST in the United Kingdom.

2 ADOPTION AND IMPLEMENTATION OF TIBER-IT

TIBER-IT has been formally adopted by the Authorities, and the ECB and TKC members have been officially informed about its launch; they are informed on a continuous basis on TIBER-IT implementation.

The Authorities promote the voluntary participation of financial entities in TIBER-IT tests, and they steer the annual and multi-annual planning by consulting the financial entities that have expressed their intention to be tested.

TIBER-IT activities are organised in detail in calendar periods, lasting approximately one year each. The deadline for enrolment takes into account the annual budgeting and planning cycle of financial entities in order to give them the possibility to include the TIBER-IT test in their annual planning. There is no fee for participation.

Financial entities decide to participate on a voluntary basis and allocate resources to scope, steer and report their testing activities to the relevant stakeholders, as envisaged in this Guide. The decision to participate in the test should be taken by the entity at Board level.

The Authorities are responsible for providing guidelines and support for the deployment of TIBER-IT. For these tasks, the Authorities have set up a TIBER Cyber Team (TCT, §3.2.2): it facilitates the execution of the test, among other things, for ensuring the mutual recognition of the test by other relevant authorities. The TCT liaises with the TKC and with the TCTs of other authorities and/or countries.

The TCT, with the support of other stakeholders, delivers and updates the GTL report, which aims at supporting the financial entities dealing with the threat intelligence phase of the TIBER-IT testing process.

Targeted threat intelligence and red teaming services should be procured by the entity, following the instructions detailed in the TIBER-EU Services Procurement Guidelines.[11] The procured Threat Intelligence (TI) Provider should leverage, if available, the GTL in order to deliver the Targeted Threat Intelligence (TTI)[12] Report to the tested financial entity.

More details on the roles and responsibilities of TIBER-IT actors are in §3.2.

2.1 TIBER-IT: SCOPE

The TIBER-IT has been adopted with a gradual approach and it is primarily addressed to critical financial entities in order to improve the cyber resilience of the single entity and, at the same time, reduce any adverse effects that an incident may cause to the financial sector as a whole.

Specifically, the target group includes the following entities operating in Italy:

---

11 https://www.ecb.europa.eu/pub/pdf/ecb.tiber_eu_services_procurement_guidelines.en.pdf

12 The TTI Report provides detailed insight into the entity's attack surface and its defence posture (see § 3.5.1).

- financial market infrastructures;
- payment systems and supporting technological or network infrastructures;
- trading venues;
- banks;
- payment and electronic money institutions;
- financial intermediaries (pursuant to Article 106 of the TUB);
- insurance undertakings and intermediaries.

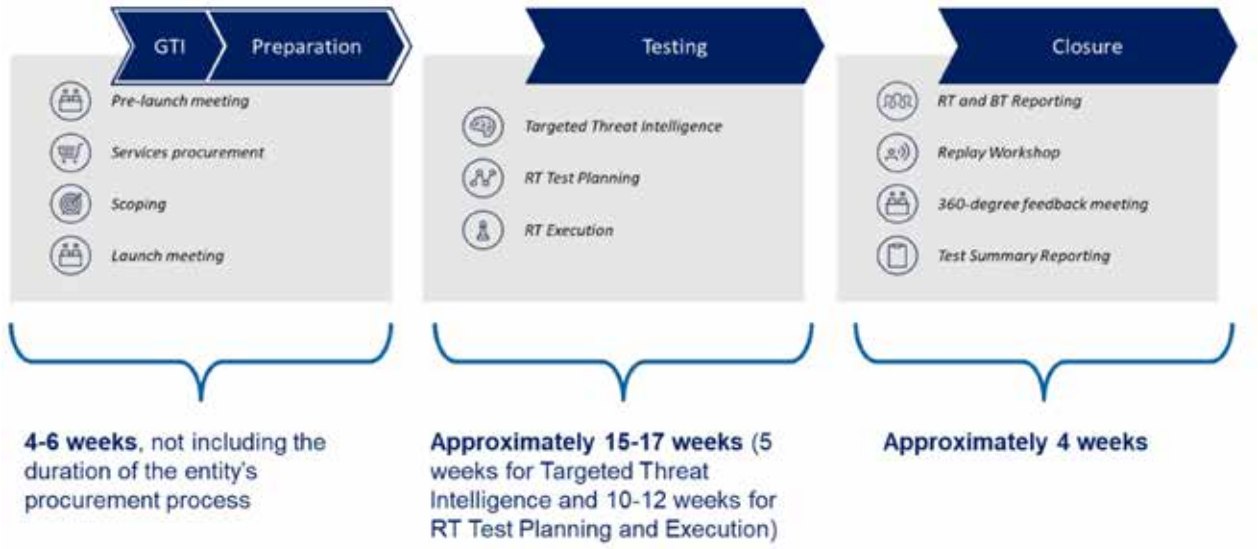
However, the definition of a main target group of entities to which TIBER-IT is primarily addressed does not preclude the possibility to be flexible in allowing the evaluation of TIBER-IT tests on a type of entity not already included in the list, on a case-by-case basis and taking into account its interconnections with other financial entities and its cyber maturity.

3 HIGH-LEVEL OVERVIEW OF THE TIBER-IT PROCESS

3.1 TIBER-IT PROCESS OVERVIEW AND KEY PHASES

The overall TIBER-IT test process consists of three main phases: i) preparation, ii) testing, and iii) closure (Figure 2) and is fully aligned with the process outlined in the TIBER-EU framework.

Figure 2: OVERVIEW OF THE TIBER-IT PROCESS: MAIN PHASES AND ACTIVITIES



The preparation phase starts with a pre-launch meeting, which is followed by external service procurement and scoping, and leads to a launch meeting.

The testing phase starts with the gathering of the targeted threat intelligence by the TI provider and the red teaming planning and execution by the Red Team (RT) provider.

After the completion of the red teaming test, the closure phase starts with RT and Blue team (BT) reporting, followed by a replay workshop, a 360-degree feedback meeting and test summary reporting.

To foster the harmonisation and standardisation of the approach to threat intelligence based ethical red-teaming across the EU, the documentation produced by the tested entity during the TIBER-IT test execution should be in line with the TIBER-EU templates and, if deemed necessary, customised by the Authorities in order to take into account national specificities. The reference documentation is available respectively on the ECB website and on the Bank of Italy website section dedicated to TIBER-IT.[13]

[13] The TIBER-IT section is available on the Bank of Italy's website at: Home/Our Role/Market and Payment System Oversight/TIBER-IT

3.2 TIBER-IT KEY ACTORS, ROLES, RESPONSIBILITIES AND INTERACTIONS

This section describes the main actors, roles, responsibilities and interactions among the main stakeholders involved in both management and implementation activities of the TIBER-IT framework. The key stakeholders involved in a TIBER-IT test are the:

- TIBER-IT Steering Committee (TIBER-IT SC);
- TIBER Cyber Team (TCT) and Team Test Manager (TTM);
- White Team (WT) and White Team Lead (WTL);
- Blue Team (BT);
- Targeted Threat Intelligence (TI) provider;
- Red Team (RT) provider.

All the main stakeholders of a TIBER-IT test should be well informed about their respective roles and responsibilities to ensure that:

- the test is conducted in a controlled manner by adopting a risk-based approach;
- a clear protocol is set out for the information flows among the relevant stakeholders throughout the test;
- the information flows protocol clearly defines how information is stored and shared among the relevant stakeholders.

To further clarify the roles and responsibilities of the different stakeholders involved in the overall process of a TIBER-IT test, a Responsibility Assignment (RACI) Matrix is included in Annex I 'TIBER-IT RACI Matrix and main deliverables'.

3.2.1 TIBER-IT Steering Committee (TIBER-IT SC)

A TIBER-IT SC, comprising Bank of Italy, Consob and IVASS representatives, will be established as a crossauthority high-level committee responsible for coordinating TIBER-IT maintenance and implementation and steering the annual and multi-annual testing programme. The TIBER-IT SC will be chaired by a senior manager from one of the Authorities involved.

It will support the competent bodies of the Authorities in communicating the completion of the test by the entity, according to the process envisaged in TIBER-EU and in these guidance requirements.

The TIBER-IT SC may be consulted by the TTM with regard to the invalidation of the test if it is not recognised as a TIBER test, in the event that the entity is not conducting the test in the spirit of the TIBER-EU framework and according to the requirements of the TIBER-IT National Guidance.

3.2.2 TIBER Cyber Team (TCT) and Team Test Manager (TTM)

The TCT comprises representatives from the financial authorities adopting this guidance and is supported by a stable pool of resources provided by

the Financial System Operational Resilience Division of the Bank of Italy's Directorate General for Markets and Payment Systems.[14]

The TCT acts as the contact point[15] for any enquiry with regard to TIBER-IT and to cross-border TIBER tests; it manages and leads the implementation and proposes updates to TIBER-IT in the Italian financial sector, in close collaboration with other relevant national authorities. The TCT supports the planning and coordination for the execution of TIBER-IT tests.

The TCT facilitates TIBER-IT tests across the financial sector, and provides support and specialist knowledge to WTLs. It also facilitates dialogue among all the relevant stakeholders including, when deemed appropriate, supervision and oversight functions.

The TCT liaises with other TCTs in other TIBER jurisdictions and with the members of the TKC on a continuous basis.

A Team Test Manager (TTM) is appointed for each TIBER-IT test as the main point of contact for the WT and it is responsible for verifying that the entity undertakes the test in a uniform and controlled manner, in accordance with this guidance. It is supported in its duties and tasks by the TCT. Given the importance of the TTM's role, an alternate TTM may also be appointed.

If an entity does not conduct a TIBER-IT test in the spirit of the TIBER-EU framework and according to the requirements of the TIBER-IT National Guidance, the TTM may propose the invalidation of the test to the TIBER-IT SC, which supports the competent bodies of the Authorities in invalidating a test not recognised as a TIBER test.

The TTM also plays a pivotal role in the event of significant deviations from the original planning. These should be discussed by the WT with the TTM.

The TTM should agree on the scope and the scenarios, and ensure that the test is executed according to the plan and that it conforms to TIBER-IT test standards and all the relevant requirements, which is important for mutual recognition by other jurisdictions.

Since all parties involved in a TIBER-IT test should take a collaborative, transparent and flexible approach, close cooperation between the TTM and the WTL is required during all phases of the test process. In particular, the TTM should also have direct access to the TI and RT service providers when required. Moreover, where there are crucial decisions to be made or where differences of opinion arise, both the TTM and the WTL should have a formal escalation line to their respective superiors and/or decision-making bodies. For the financial entities, these formal lines may consist of the entity's chief information security officer, chief operating officer, chief risk officer or any other appropriate senior personnel with sufficient decision-making authority.

---

14 This Division is exempt from any direct supervision or oversight responsibilities.

15 The following email address tiber-it@bancaditalia.it is a single point of contact for any enquiry regarding the TIBER-IT framework.

The TTM is independent of the WT and is not accountable for the WT's actions, the running of the test, the outcomes or the remediation planning.

3.2.3 White Team (WT) and White Team Lead (WTL)

For each TIBER-IT test, the entity should establish a WT, led by a dedicated WTL. The WT is responsible for: scoping and running the test, service procurement and engaging with all other parties, and remains accountable for the management of risks during the test.

The WT should be composed of personnel with adequate knowledge of the CFs tested and of senior management from the entity, positioned at the top of the security incident escalation chain. People in the WT shall be the only ones aware of the TIBER-IT test within the organisation, thus the WT should be kept as small as possible to ensure that knowledge of the test is minimised.

This team is responsible for the overall planning and management of the test, in accordance with the TIBER-IT National Guidance and the TIBER-EU framework.

The WTL coordinates all test activities, including engagement with the TI and RT providers and possible meetings with the authorities.

More details on the roles, responsibilities and ideal composition of the WT can be found in the TIBER-EU White Team Guidance.[16]

3.2.4 Blue Team (BT)

For each TIBER-IT test, the BT is composed by all other (non-WT) personnel of the entity being tested, including third parties, especially those who manage systems (and the people, processes and technology involved) of the entity being tested. In particular, the BT also includes the staff responsible for defending the entity's information systems by assuring its security posture against a group of cyber-threat actors. It is crucial that the BT be unaware of the test for its duration and completely excluded from the preparation and conduct of the TIBER-IT test.

Only during the closure phase will the BT be informed about the test, and the main members of the BT should participate in the replay and follow up activities. During the closure phase, the BT is responsible for drafting the BT report, a technical report that covers the defence actions performed by the BT during the RT's actions, for each threat scenario being tested.

3.2.5 Threat intelligence (TI) provider

The TI provider is an external provider procured by the WT according to the standards and minimum requirements established in the TIBER-EU Services Procurement Guidelines. The TI provider gathers targeted intelligence on the entity, emulating the research that would be performed by an advanced cyber attacker, and provides this information to the entity in the form of a TTI

16 https://www.ecb.europa.eu/pub/pdf/other/ecb.tibereu.en.pdf

Report. TI providers should use multiple sources of intelligence to provide an assessment that is as accurate and up to date as possible.

The TI provider works in close cooperation with the RT provider, by helping to develop the attack scenarios for the red team test, as well as any new intelligence requirements that occur as the red team test progresses. The TI provider is expected to provide input for the final report issued to the entity.

3.2.6 Red Team (RT) provider

The RT provider is an external provider, procured by the WT, according to the standards and minimum requirements set out in the TIBER-EU Services Procurement Guidelines[17]. Its goal is to attempt to breach the security safeguards of the entity, by following a rigorous and ethical red teaming methodology, always within the boundaries of the TIBER-IT National Guidance and the TIBER-EU framework. The rules of engagement and the specific testing requirements should be established by the RT provider and the entity.

The RT provider drafts the Red Team Test Plan and executes a TIBER-IT test on the targeted systems and services, which were agreed in the scope (see §3.5). After the completion of the testing phase, the RT provider prepares a review of the test and any issues arising and drafts a Red Team Test Report.

The RT provider works closely with the TI provider during all the phases of the test in order to update the threat intelligence assessment and attack scenarios with relevant and up-to-date intelligence. Lastly, the RT provider is expected to liaise with the TI provider in order to design and deliver the Red Team Test Report issued to the entity.

3.3 Risk management in the execution of TIBER-IT tests

TIBER-IT testing is conducted on the live production systems that underpin the critical functions of an entity, taking into account the real attack surface and the actual weaknesses of the entity. Therefore, the execution of the test involves potential risks. Consequently, appropriate risk controls must be applied to ensure that the testing activities do not cause any harm to the financial entity's operations[18] or to its customers.

As part of the risk management, the WT may halt the test at any point, if it considers that continuing the testing poses an unacceptable risk to the entity. The WT should ensure that appropriate risk management and controls are communicated and understood by all the relevant stakeholders, taking into account the internal control framework and governance of the financial entity.

---

17 https://www.ecb.europa.eu/pub/pdf/other/ecb.1808tiber_eu_framework.en.pdf

18 In accordance with the widely adopted TLPT effective practices and the *G7 Fundamental Elements For Threat-Led Penetration Testing (2018)*, in conducting TIBER-IT tests, financial entities, in consultation with their relevant stakeholders, should apply effective risk management controls to reduce the risk of any potential impact on entity data, damage to entity assets and disruption to critical services and/or operations at the entity or in the financial sector.

The functions and information systems targeted in TIBER-IT testing contain information protected by several legal acts, such as confidential banking information, electronic communications and personal data. Therefore, every effort must be made to maintain the integrity, availability and confidentiality of this information by adequate risk management means throughout the test and to comply with these legal acts.

In light of the above, a risk assessment must be conducted by the entity before the test to ensure that the right processes, procedures and controls are taken in line with the entity's existing risk management framework. The WT will develop a risk management plan for the testing, in order for risks to be identified, analysed and mitigated according to the entity's practices regarding risk management. The risk management plan, which must be updated with any significant changes, will include at least:

- what kind of tactics, techniques, and procedures (TTPs) cannot be used;
- what functions, systems and other potential targets are outside the scope of testing;
- what contingency measures have been taken and how the WT would react in the event of potential disruptions caused by the test.

The WT is responsible for ensuring that the RT prepares its testing plan within the boundaries of this risk assessment.

The WT, the TI provider, and the RT shall agree on a project codename to be used in all documentation throughout the test, in order to protect the identity of the financial entity and the nature of the test.

With the aim of protecting the confidentiality of the test, the WT must limit awareness of the test to a small trusted group within the entity, whose members have the appropriate levels of seniority to make risk-based decisions regarding the test.

The TI provider and the RT must agree with the WT on the procedures for handling and protecting information during the test and for deleting it after the test (see also §3.4.2).

To manage risks effectively during the test, the WT must remain in control of the testing process to ensure that the test proceeds in accordance with the scope, scenario, planning and process agreed.

3.4 Preparation phase

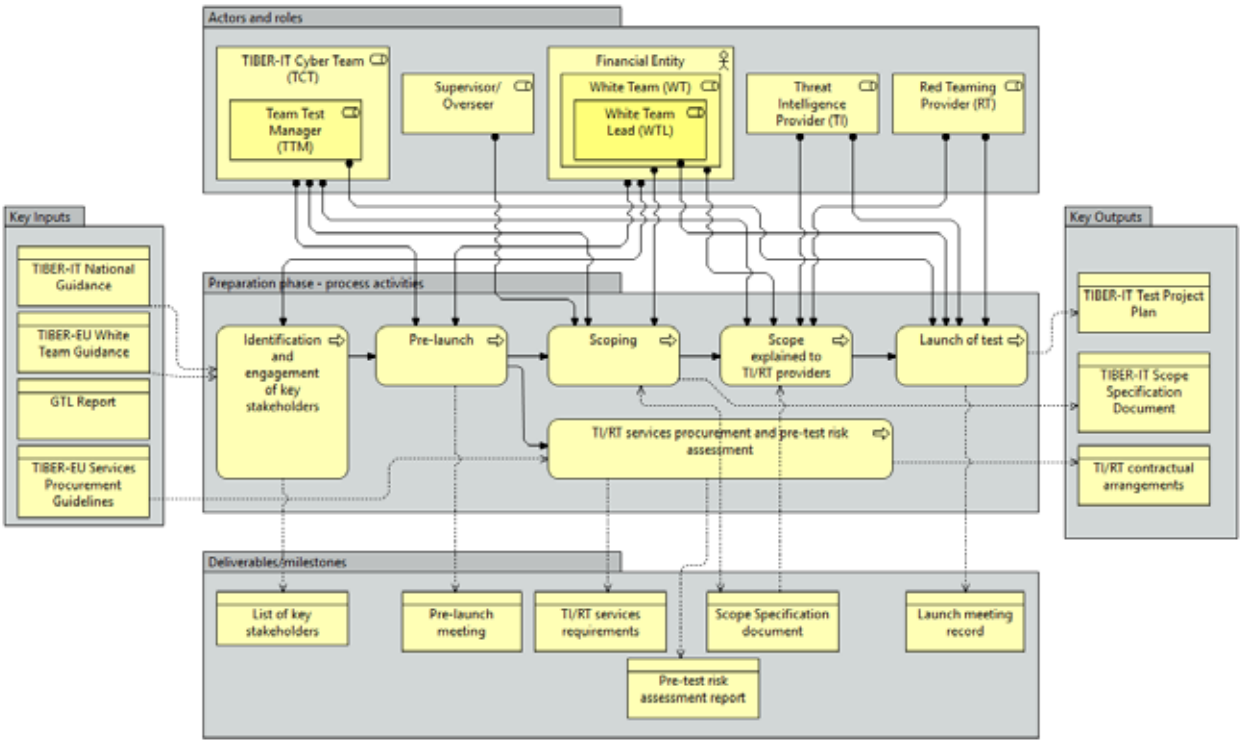
During the TIBER-IT preparation phase, the commitment to the TIBER-IT test is formally launched. The TTM starts collaborating with the participating entity. The scope of the test is established and the entity procures the TI and RT providers. This preparation phase lasts approximately four to six weeks, not including the duration of the entity's procurement process.

At the beginning of the preparation phase, the TCT requests the nomination of a WT and a WTL by the entity. The WT comprises a small number of senior individuals who are experts and/or in the position of making risk-based decisions throughout the test. Once established, the entity informs the TCT of the composition of the WT. The WTL ensures that the WT is aware of the

TIBER-IT test, of the requirement for maintaining secrecy and of the process the team should follow in case certain situations arise (e.g. in the event that the BT detects the simulated attack and escalates a TIBER-IT-related incident).

The preparation phase starts with a pre-launch meeting, which is followed by service procurement and scoping, and leads to a launch meeting (Figure 3).

Figure 3: OVERVIEW OF THE TIBER-IT PROCESS – PREPARATION PHASE



3.4.1 PRE-LAUNCH MEETING

The WTL holds the pre-launch meeting with the TTM and any additional WT members that the WTL wishes to invite. Further guidance for the WT is detailed in the TIBER-EU White Team Guidance and in the TIBER-EU Services Procurement Guidelines, which can be discussed during the meeting.

During the pre-launch meeting, the TTM should brief the entity on the requirements for:

- the testing process in the TIBER-EU framework and its further contextualisation as envisaged in this TIBER-IT National Guidance;
- the stakeholders' roles and responsibilities;
- the security protocols (including secure document transfer);
- contractual considerations (including sharing documentation from TI/RT providers);
- project planning.

To facilitate the free, safe and secure flow of information, participating parties – including the WT and TI and RT providers – should sign a non-disclosure agreement (NDA).

A date for the launch of the test should be set at this point.

3.4.2 Services procurement

After, or even possibly in parallel with the pre-launch meeting, the WT starts the procurement process. The TCT exercises a degree of judgement over whether to allow the WT to start the procurement process in parallel with the pre-launch or whether to allow it to do so only once the pre-launch and scoping have been completed.

Given the sensitive nature of TIBER-IT tests, the TI and RT providers must undergo a rigorous due diligence process based on selection criteria, aimed at verifying that the external provider is able to provide highly skilled professionals specialised in conducting advanced ethical hacking activities. Some of these criteria include the professional references in the threat intelligence and ethical hacking fields, the level of expertise of the personnel to be involved in tests, the adherence to a code of conduct and an adequate level of assurance.

In particular, since the WT is responsible for the sourcing of the TI and RT testing services, they must be procured by following the indications and the minimum requirements detailed in the TIBER-EU Services Procurement Guidelines.

More specifically, as tests are conducted on live production systems, the WT must procure the most competent, qualified and skilled TI and RT providers with the requisite experience to conduct such tests, in order to avoid risks due to unexperienced or unskilled service providers.

A TIBER-IT test must be conducted by independent third party providers, thus excluding the possibility of utilising internal resources. Where feasible, entities should ensure that the providers procured are accredited and certified by a recognised body as being able to conduct a TIBER-IT test. The TTM will provide consultation as required on procurement matters.

During procurement, the WT should carry out the following activities:

- ensure adherence to the TIBER-EU Services Procurement Guidelines and to best practices to identify potential TI/RT providers capable of meeting the objectives of the test;
- issue a request for proposal (RFP) in compliance with the TIBER-IT National Guidance and with any relevant procurement legislation;
- assess RFP responses, and then interview and select appropriate providers and,
- establish conditions governing the sharing, confidentiality and retention of intellectual property rights.

When procuring the TI and RT service providers, the WT should ensure that there is a mutual agreement on at least the following aspects: the scope of the

test; boundaries; timing and availability of the providers; contracts; actions to be taken and liability (including insurance where applicable).

The contracts between the WT and the TI and RT providers should include, among other things:

- security and confidentiality requirements that are at least as stringent as those followed by the entity tested as regards confidentiality requirements;
- provisions for appropriate protection measures;[19]
- a clause relating to non-disclosure and confidentiality, data handling, data protection and destruction requirements and breach notification provisions and,
- activities not allowed during the test, such as destruction of equipment; uncontrolled modification of data/programmes; jeopardising the continuity of critical services; blackmail; threatening or bribing employees and disclosure of test results.

Once procurement has been completed, the WT attests that, to the best of their knowledge, the procurement process has adhered to both the TIBER-EU White Team Guidance and the TIBER-EU Services Procurement Guidelines.

3.4.3 Scoping

The key objective of scoping is for the WT and the TTM to agree on the scope of the TIBER-IT test and on the identification of the CFs, which must be included in the scope. The entity may decide at its discretion to include additional non-critical functions (i.e. people, processes and technologies) within the scope of the test, provided these do not negatively affect the testing of the CFs. The scope of the TIBER-IT test will usually also include the systems, people and business processes underpinning the entity's CFs that are outsourced to third parties.

For the purposes of a TIBER-IT test, the relevant testing activities must be performed on the entity's live production systems. However, the entity may also include pre-production, testing, backup and recovery systems within the scope of the TIBER-IT test.

For the purposes of scoping, both the TTM and WT should have extensive knowledge of the entity's business model, functions and services.

The WT should conduct a business impact analysis defining the CFs as part of their standard operational risk management practices. While identifying the CFs and the scope of the test, the WT may also refer to the GTL Report to provide extra context to its business and the threats to be dealt with, and to map the possible threat scenarios to its CFs. The TTM, with the help of the TCT, will consult with the relevant supervisors to make sure that all appropriate CFs are considered in the scoping.

[19] E.g., insurance policy for the activities of IT and RT Providers not previously envisaged in the contract and/or resulting from fraud, negligence and so on (see also TIBER EU Services Procurement Guidelines).

A draft TIBER-IT Scope Specification document[20] must be prepared and distributed by the WT before the Scoping meeting. This document identifies the scope of the TIBER-IT test and also details which key systems and services underpin each CF. Using this information, the WT sets the 'flags'[21] to be captured by the RT during the test, which must be discussed with and approved by the TTM. These flags can, however, be modified on an iterative basis during the test, following TI gathering and the evolution of the test; in such cases, the risk assessment plan (see §3.3) should be updated too.

The final TIBER-IT Scope Specification document should be agreed with the TTM during a Scoping meeting organised by the WT for all the relevant stakeholders (e.g. WT, TTM and possibly the TI/RT providers). It is fundamental that the scope of the TIBER-IT test is agreed and signed by the entity's Board.

If the procurement phase has been concluded, the scoping process and meeting may include the TI/RT providers. Otherwise, it is recommended that the WT and TTM discuss this in advance of the scoping meeting and another meeting with the TI/RT providers should be planned to explain the CFs and the systems underpinning them.

3.4.4 Test launch

The Launch meeting is a meeting that should involve all the relevant stakeholders (including the TTM, WT and TI/RT providers), whose agenda includes the test process and expectations, as well as the draft TIBER-IT Project Plan. The purpose of the Launch meeting is to agree on responsibilities and to schedule the planning and the execution of the TIBER-IT test.

Once the procurement process has been completed and all the relevant contractual arrangements are in place, the WT must prepare a draft project plan. This must include a schedule of meetings to be held between the WT, TI/RT providers and the TTM. The project plan must be distributed to all stakeholders by the WTL before the Launch meeting. The TIBER-IT project plan covers:

- testing organisation and logistics;
- objectives for the test in relation to the GTL report;
- tested functions and underlying people, processes and technology;
- schedule for preparations and testing;
- specific objectives;
- boundaries;
- risk management;
- communication during testing;

---

20 Based on the TIBER-EU Scope Specification template: https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/shared/pdf/Final_TIBER-EU_Scoping_specification_template_July_2020.pdf

21 The 'flags' are substantially the targets and objectives that the RT providers must attempt to capture during the test, using a variety of techniques.

- other practicalities for the testing.

A code name for the entity must be chosen and used by all stakeholders when referring to the entity during all the phases of the test process to ensure the confidentiality and secrecy of the test.

3.5 Testing phase

The Testing phase should start once the scope has been agreed, the TI/RT providers have been engaged and all the stakeholders have been informed about their roles and responsibilities.

The Testing phase involves TI gathering on the tested entity, thanks to which detailed threat scenarios are developed by the TI provider. The RT will build upon these and develop attack scenarios to create the TIBER-IT Red Team Test Plan[22] before the test execution.

The TTI Report is needed to develop threat intelligence-based scenarios mimicking real life cyber-attacks, and the GTL Report, if available, should be used. While the GTL Report reproduces the most significant threats faced by the financial sector, it can be used as valuable input to develop the TTI Report, which gives a detailed view of the specific entity's attack surface and current defences. Moreover, the TTI Report supports the development of viable and realistic attack scenarios by emulating the TTPs of real life threat actors, leading to the delivery of a realistic simulation.

The GTL Report for the Italian financial sector is provided by the TCT,[23] while the TTI Report is prepared by the TI provider. The GTL Report may be updated by the TCT on an ongoing basis, at least annually, as new threat actors, TTPs and vulnerabilities emerge.

The Testing phase continues with the handover between the TI and the RT providers; this activity is followed by the development of the Red Team Test Plan and the attack scenarios, and leads to the execution of test.

3.5.1 Targeted Threat Intelligence (TTI) and Threat Scenarios Identification

If the GTL Report is available, the TI provider should connect it to the TTI Report to develop specific threat scenarios for the targeted entity. In doing so, the TI provider should consult the RT provider to ensure the developed scenarios are viable (Figure 4).

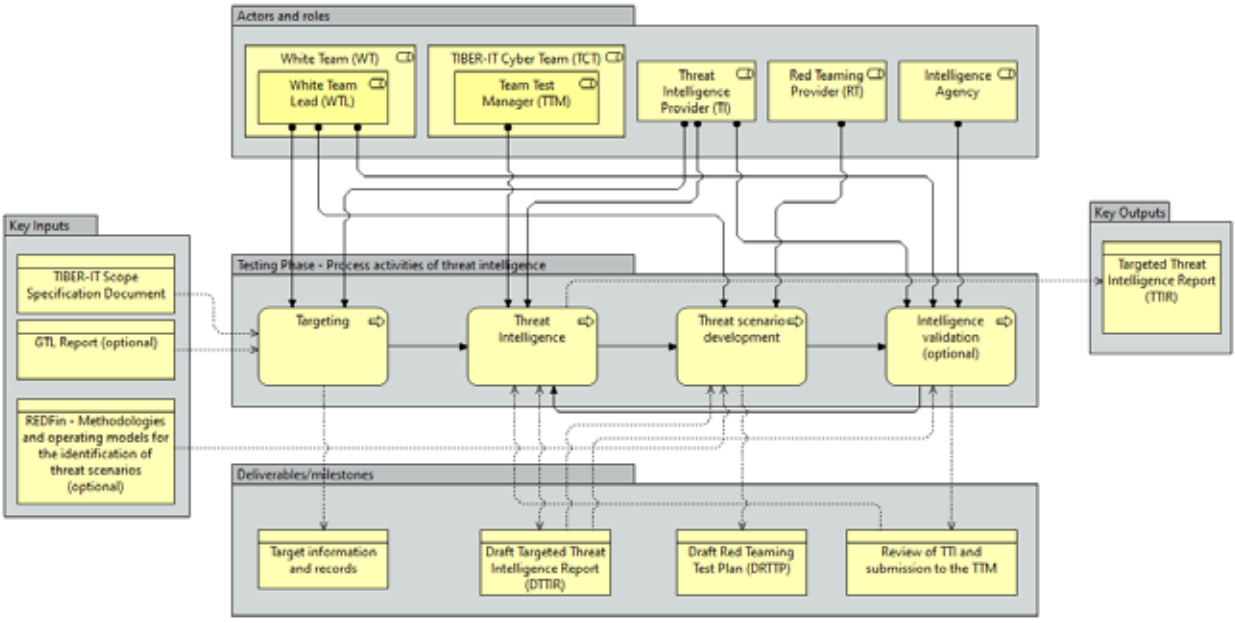
During the TTI process, the TI provider collects, analyses and disseminates CF-focused intelligence relating to two main areas of interest:

---

22 https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/shared/pdf/Final_TIBER-EU_Guidance_for_the_Red_Team_Test_Plan_July_2020.pdf

23 Under the coordination of the TCT and based on specific arrangements, the GTL Report may be drawn up in close collaboration with the other relevant stakeholders. In particular, the TCT might leverage the support provided by other financial authorities, corporate cyber security and risk governance functions, the CERTFin and other Intelligence and security agencies.

Figure 4: OVERVIEW OF THE TIBER-IT PROCESS – TESTING PHASE – TTI PROCESS



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

The TI provider uses information provided by targeting and threat intelligence identification activities, combined with the optional valuable inputs provided by the WT, to develop threat scenarios.

The targeting activity is performed by the TI provider to achieve a detailed preliminary picture of the entity and its weaknesses from the attacker's perspective. The outcome of this activity is the identification, on a CF-focused and system-by-system basis, of the attack surfaces of the people, processes and technologies relating to the entity, and of its global digital footprint. This may include information that is intentionally published by the entity and other internal information that has been unintentionally leaked, such as customer data, confidential material or other information that could be a useful resource for an attacker.

Targeting activities are a valuable input and a core element of the TTI Report, with the aim of tailoring the threat profile and scenarios. Since targeting makes known some of the entity's attack surfaces and identifies initial targets, it also is a valuable input for subsequent RT providers' deeper and more focused targeting activities.

Concerning threats activities, the TI provider collects, analyses and disseminates intelligence about significant threat actors and probable threat scenarios, with the objective of presenting a credible picture of the cyber threat landscape, based on evidence-backed threat intelligence which is specifically tailored to

the entity's business environment, including critical third party providers. The TI provider may use the GTL Report to further integrate the identification of threats.

The output resulting from the threat identification process is a summary of the main threats, detailed profiles of the threats with the highest scores, and potential scenarios in which a high-scoring threat actor might target the entity.

In order to make intelligence gathering as efficient as possible and to ensure that it is relevant to the scope of the testing and the entity's business, the WT should provide the TI provider with a completed input for the targeted threat intelligence, which covers:

- a business and technical overview of each system supporting CFs in the scope of the test;
- the current threat assessment and/or threat register;
- any example of recent attacks.

The whole TTI process lasts approximately five weeks.

The TTI process' output is the TTI Report which is a bespoke and focused threat intelligence report for the entity being tested. Its aim is to use specific targeted threat intelligence and reconnaissance relating to the entity, taking into consideration the real-life actors within the threat landscape, to help develop attack scenarios. The TI provider is responsible for the development and production of the TTI Report[24] and makes it available to the RT provider, which uses the content of the TTI Report to develop the attack scenarios into a Red Team Test Plan. The TTI Report constitutes a strong evidential basis for the proposed red team test. In this respect, three outputs are particularly important:

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

To create realistic threat scenarios describing attacks against the entity, these scenarios have to be based on the evidence available on real-world threat actors, together with other intelligence data on the entity. The adoption of various practices of intelligence gathering and analysis is warmly encouraged. Moreover, a structured approach based on standardised methodologies and operating models for the identification of threat scenarios is recommended.[25]

The TI provider must always demonstrate strong ethical behaviour and TTI activities must always be conducted in compliance with the applicable laws.

---

24 https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/shared/pdf/Final_TIBER-EU_Guidance_for_Target_Threat_Intelligence_July_2020.pdf

25 To facilitate the identification of realistic threat scenarios, financial entities might refer to and leverage the ABI Lab REDFin document 'Methodologies and operating models for the identification of threat scenarios'.

Real-life cyber attackers may not have time or resource constraints like those placed on the TI/RT providers, having the possibility to spend months preparing an attack and not being restrained by moral, ethical and legal boundaries. Similarly, the systems underpinning the CFs typically do not have a large footprint on the public internet. Whether they are internal bespoke systems or external systems that span multiple organisations with common connecting infrastructures, the knowledge of TI/RT providers of how these systems function may be limited compared with real-life cyber attackers with the capacity and time to study them extensively.

Therefore, the entity should determine how much information it is willing to divulge to TI/RT providers, to ensure that they have the proper level of knowledge to simulate advanced attacks. In this way, TIBER-IT would reflect a 'grey box' testing approach in contrast with a 'black box' approach.

Experience shows that the more relevant information an entity gives to the TI/RT providers, the more the participating entity will gain from the test. If the entity has an internal threat intelligence capability or function and the secrecy of the test can be maintained, the TI provider may coordinate with it to gather relevant information that will support the development of the TTI Report.

Once the draft TTI Report is completed, the TI provider should share it with the WT, the TTM and the RT provider and to jointly undertake a thorough review of it, in order to correct any factual errors and to discuss any issues that may arise. Building upon the draft TTI Report, the WT and the TTM may decide to update or modify the flags established during the Scoping phase. The TTI report should be shared with the abovementioned stakeholders well before the handover meeting between the TI and the RT providers. Moreover, when necessary, the national security and intelligence agencies deemed relevant for each test might be contacted by the TTM to give feedback on the draft TTI Report.

The development of the attack scenarios is the key transition point between the TI and RT providers. This activity is carried out either just before or in parallel with a possible evaluation of the draft TTI Report by any security or national intelligence agency.

The RT provider should develop and integrate the attack scenarios into a draft Red Team Test Plan, using the scenarios included in the draft TTI Report, and in line with the TIBER-IT Test Scope Specification document. At this stage, a workshop may be held, between the WT, the TTM and the TI/RT providers, to review the scenarios presented by the TI provider and to enable the Red Team Test Plan to be developed by the RT provider.

The workshop activities include:

- an overview of the TTI Report and the potential changes following any feedback from security and national intelligence agencies;
- feedback comments on the TTI Report by the TTM;

- presentation of the draft Red Team Test Plan, including CF scenario mapping, flags, possible anticipated leg-ups,[26] risk mitigation, escalation procedures, test start/stop dates and a draft Red Team Test Report delivery date, provided by the RT provider.

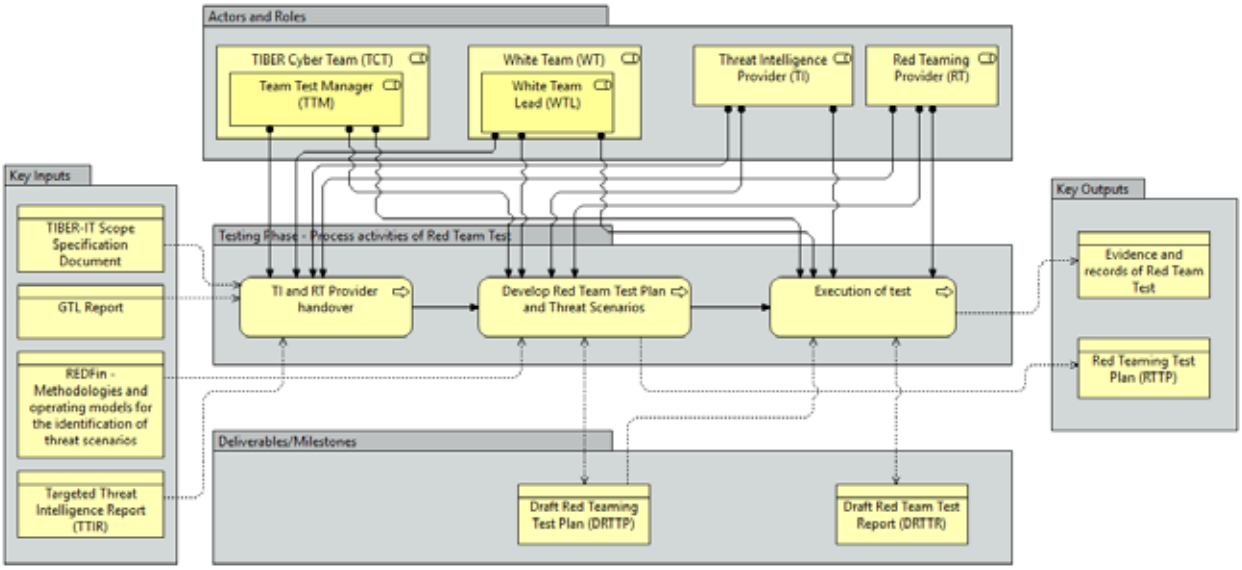
After the workshop, the TI provider should update and produce a final version of the TTI Report to be delivered to the entity. Similarly, the RT provider should also update the draft Red Team Test Plan in the light of the workshop findings and the risks identified.

It is forbidden under any circumstances for the TI/RT provider to use any of this threat or risk information in any other context outside the testing assignment either individually or in aggregated form. The TTI Report is highly confidential and it is necessary to protect its contents from being leaked outside this limited group of stakeholders, including within the entity's BT.

3.5.2 Red team test planning

Once the TTI process is completed, the RT provider plans and executes the TIBER-IT test on the target systems and services that underpin each CF in the scope of the test (Figure 5).

Figure 5: OVERVIEW OF THE TIBER-IT PROCESS – TESTING PHASE – RT PROCESS



This phase needs to allow sufficient time for the RT provider to conduct a realistic and complete test, in which all attack phases are performed and all test objectives and flags – agreed during the scoping phase and updated

[26] If during the testing process the RT provider is unable to progress to the next stage due to time constraints or because the BT has been successful in protecting itself, the RT provider, in agreement with the WT and TTM, may be given a 'leg-up', whereby the WT essentially gives the RT provider access to its system, internal network and so on, to continue with the test and focus on the next flag/target to be achieved.

during the TTI process – are achieved. The time allocated for testing should be proportionate to the scope, the entity's resources and the availability of the supporting information supplied by the WT. In general, 10-12 weeks is an appropriate amount of time for testing.

Before the start of the test, a TI/RT handover session is held, to provide a detailed explanation of the TTI Report and to discuss possible threat scenarios for the testing. Following the TI/RT handover meeting, the RT provider should further build on the TIBER-IT Scope Specification document, the GTL Report and the TTI Report to integrate the attack scenarios and finalise the Red Team Test Plan.

The RT provider should deploy a broad range of TTPs during the test, by using test methodologies such as reconnaissance, weaponisation, delivery, exploitation, control and movement and actions on the target.[27]

In preparing the attack scenarios and the Red Team Test Plan, the RT provider should:

- align its test objectives with the goals of each of the actors;
- map the objectives and goals that support the CFs;
- produce credible real-life attack scenarios for the test;
- design the attack scenarios to provide background to the tradecraft employed by each threat to conduct a successful attack;
- adapt its attack methodology to emulate the real-life attack scenarios;
- draw upon the TTI Report, which reveals some of the entity's attack surfaces, as a basis for deeper and more focused targeting activities;
- add some elements which test the detection and response capabilities of the BT;
- indicate, in coordination with the WT, where a 'leg-up' might be needed if the attack is not successful;
- include an appropriate plan for managing the risks the red team test poses to the target system and the business information associated with it;
- avoid any action that may have destabilising effects on financial stability or on the operational resilience of the Italian financial system.

The output of the test planning is the final Red Team Test Plan, which includes the attack scenarios to be performed and the risk management controls that will be applied to ensure that the test is conducted in a controlled manner.

The attack scenario writing is a creative process. The attack scenarios are written from the attacker's point of view and define the flags to be captured. In the attack scenario writing, the RT provider should indicate various creative options for each of the attack phases based on various TTPs used by advanced attackers to anticipate changing circumstances or in case the first option does not work. The TTPs may not simply mimic scenarios seen in the past, but may combine the techniques of the various significant threat actors, including

[27] Please refer to TIBER-EU framework for further details.

creative and innovative TTPs that have not yet been seen in the wild but are expected for the future. This is the 'Scenario X', which enables a forwardlooking perspective for possible attacks. The goal of Scenario X, which does not have to be included in the Red Team test Plan, is to hypothesise what advanced attacks can be expected in the coming future. The scenario may focus on a particular innovative TTP, not yet seen and possibly combined with societal developments that will have an impact on the entity. The focus of Scenario X however, remains on critical functions.

Considering the misalignment between real-life cyber attackers and the RT provider in terms of time and resource constraints, including moral, ethical and legal boundaries, in order to facilitate a more effective and efficient test, the WT may deliver further information to the RT provider on the scenarios, including on the targeted people, processes and systems. Thanks to this information the RT provider may gain further insights and make a better use of time. In any case, experience shows that there is a direct correlation between the relevance of the additional information the WT provides to the RT provider and the overall benefit for the entity from the red teaming test.

In addition, during the testing phase, the role of the TI provider can be enhanced, by providing continuous threat intelligence to the RT provider during the test, which may result in more useful reconnaissance and more insight into how to achieve the targets. If TI and RT providers decide to work more closely during the test, they must agree on the working and information sharing arrangements.

During the testing phase, it is recommended that the WT and the RT provider agree on a regular way to monitor the progress, for example through weekly status updates (Weekly test meetings or updates), while potentially critical vulnerabilities and other security problems must always be reported without delay.

The WT may interrupt testing at any time, in which case the RT must immediately stop all its testing activities.

3.5.3 Red team test execution

The execution of the TIBER-IT test must be calibrated according to the complexity of the test. Bearing in mind the dynamic and evolving nature of threats, it is recommended that the TTI report should be used in a short timeframe for developing attack scenarios.

During the execution timeline, the RT provider should perform a stealthy intelligence-led red team test on the target systems. The RT provider can deviate from the attack scenarios within the RT Test Plan, as creativity is needed (as in real life cyber-attacks) if obstacles occur, in order to develop alternative and sophisticated ways to achieve the test objectives or flags (e.g. Scenario X).

As already mentioned, during the testing phase the RT provider may be unable to progress to the next stage, due to time constraints or because the BT has been successful in protecting the entity. In such cases, the WT and the TTM may agree to give the RT provider a 'leg-up' or steer, by giving access to systems, internal networks and so on in order to continue with the test and focus on the

next flag. All leg-ups and steers must be duly documented and reported in the RT Test Report.

During the execution of the TIBER-IT test, the RT provider should update the TTM at least once a week and keep the WT informed about progress on an ongoing basis. At this stage, meetings between the WT, the TTM, the RT provider and possibly the TI provider are strongly encouraged, since the quality of the test significantly benefits from discussion, which also helps build a relationship of trust among the stakeholders. In any cases, such meetings must be organised, conducted and kept secret as the BT must remain unaware of the ongoing test.

Regardless of the methodology used by the RT provider, the test should be conducted in a controlled manner, taking a stage-by-stage approach, and in a way that does not put the entity and its CFs at risk.

It is fundamental for the RT provider to continuously inform the WT and the TTM about progress being made at each stage, as soon as a flag or target is in sight, or at least when the RT provider has 'captured the flag'. This gives the WT the opportunity to discuss with the RT provider and the TTM what steps can and cannot be undertaken next. Furthermore, it is the moment to evaluate whether escalation procedures need to be invoked. As already mentioned, the WT can halt the test at any time, under its own evaluation. All of the RT provider's actions should be logged for replay with the BT, as evidence for the Red Team Test Report, and for future reference.

The output of the Test execution is a draft version of the Red Team Test Report[28] produced by the RT provider to be delivered to the entity. The draft report must be issued as soon as possible and no later than two weeks after the test completion, in order to ensure the quality of the Report.

3.6 Closure phase

In the closure phase of the TIBER-IT test, all the relevant stakeholders, including the BT who is finally informed about the test, reflect on the outcome of the test and make improvements to further enhance the cyber resilience of the entity being tested. This includes several tasks, among other things:

- preparation of the RT Test Report;
- drafting of the BT Report;
- execution of the RT and BT Replay workshop, possibly as a Purple Team[29] (PT);
- 360-degree Feedback meeting.

---

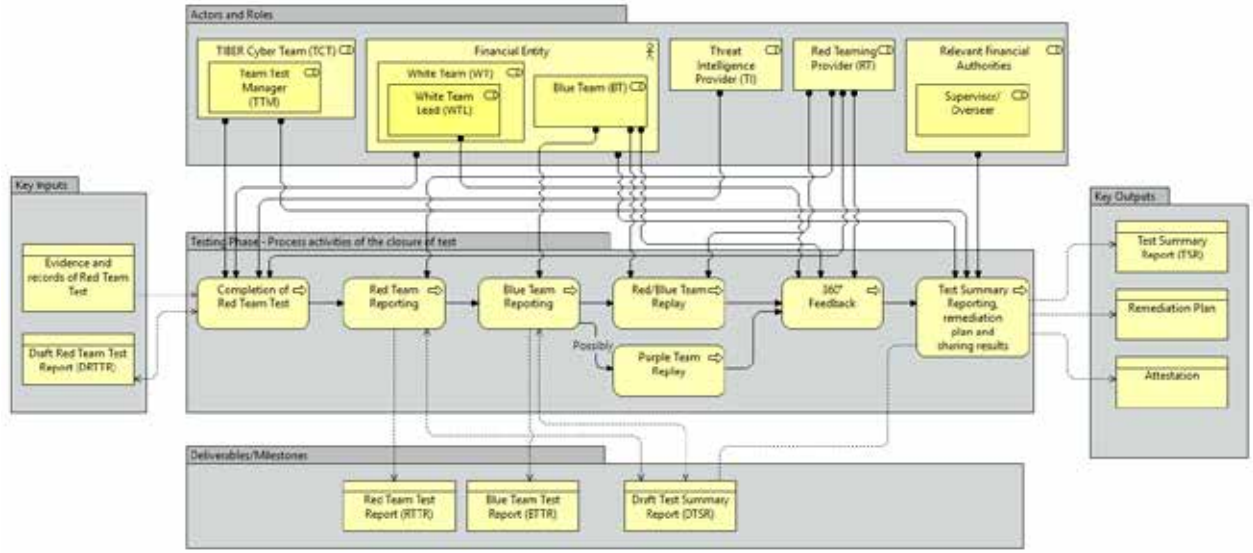
28 https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/shared/pdf/final_tiber-eu_guidance-for-the-red-team-test-report.pdf

29 The Purple Team is composed of the BT and the RT provider who work together to see which other steps could have been taken by the RT provider and how the BT could have responded to those steps. The TIBER-EU Purple Teaming Best Practices is being finalised by the ECB with a view to its publication on the TIBER-EU website: https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html

The outputs of the closure phase are: the Remediation Plan, the Test Summary Report and the Attestation. It includes as well the sharing of the results with the relevant authorities.

The closure phase starts with the completion of the Red Team Test and it is followed by the replay workshop, between the RT provider and the BT, and the 360-degree Feedback meeting. This activity is followed by the reporting of the test summary results, the definition of the remediation plan and the issuance of the TIBER-IT test attestation (Figure 6).

Figure 6: OVERVIEW OF THE TIBER-IT PROCESS – CLOSURE PHASE



In this phase, the RT provider drafts a Red Team Test Report, which includes details of the approach taken to the testing and the findings and observations from the test. The report may include advice on the areas for improvement in terms of technical controls, policies and procedures, as well as education and awareness.

During the closure phase, the attack scenarios executed during the test are replayed by the relevant stakeholders, who discuss the issues that arose during the test. Based on the findings, the entity agrees and finalises a Remediation Plan, which also includes follow-up activities, with the relevant competent authorities. Furthermore, the whole testing process is reviewed and the entity's capabilities in terms of detection and response are assessed and discussed. Finally, the key findings from the test are shared with the other relevant authorities.

The activities performed during the closure phase last approximately four weeks.

At the beginning of the closure phase, the RT provider produces a draft version of the RT Test Report, which is delivered to the entity. This Report, as previously mentioned, must be issued as soon as possible and no later than two weeks after the end of the test.

At this stage, the key members of the BT are informed about the test, and build on the RT Test Report to deliver their own BT Report. The BT Report reflects which actions the BT has undertaken during the test in comparison with the RT's actions. In order to maximise the learning from the Replay workshop, the BT Report should be completed before its date.

The RT and BT Replay workshop is organised by the entity, after the delivery of the RT Test Report and the BT Report. The purpose of this workshop is to learn reciprocally from the testing experience in collaboration with the RT provider. The replay focuses on the review of the steps taken by the BT and the RT provider during the test and it is conducted on live production systems, where feasible.

Moreover, at this stage, the BT and RT providers may work together as a PT, in order to establish which other steps could have been taken by the RT provider and how the BT could have responded to those steps.

During the workshop, the RT provider should state how far it managed to progress through the targeted attack stages of each scenario. The RT provider should also offer an opinion on what else could have been achieved if the RT had been equipped with more time and resources as genuine threat actors.

The TTM and the TI provider can also be present during the RT and BT Replay workshop.

After the workshop, the TTM should arrange a 360-degree feedback meeting between the WT, the BT, the TCT and the TI/RT providers, with the aim of jointly reviewing the TIBER-IT test to further facilitate the learning experience of all those involved in the process for future exercises. During this meeting, all stakeholders should reciprocally deliver their feedback on all the others and on the overall process; in particular, the agenda of this meeting includes:

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

In doing so, the TI and RT providers obtain feedback on their performance, and the relevant authorities have opportunities to improve the TIBER-IT process. Moreover, a 360-degree feedback report may be shared by the TCT on an anonymous basis with the TKC, to incorporate all the lessons learned from further improvements to the TIBER-EU framework, following its 'learning and evolving' principle.

After the RT and BT Replay workshop and the 360-degree feedback meeting, the entity should draft a Remediation Plan and a Test Summary Report.

The Remediation Plan is drafted by the WT with the agreement of the Board of the entity and in consultation with TI/RT providers; the TTM is informed of the plan. The Remediation Plan is based on the test results and aims at implementing corrective actions to mitigate the vulnerabilities identified during the TIBER-IT test.

The Test Summary Report[30] recaps the overall test process and results and should be based on the test documentation, such as the RT Test Report, the BT Report, the TTI Report, the RT Test Plan and the Remediation Plan. The Test Summary Report should not cover detailed technical information and findings regarding weaknesses and vulnerabilities, as this is highly sensitive information reserved for the entity alone. The Test Summary Report must be shared by the entity with the TCT, which can also review the more detailed findings from the test if it is deemed necessary.

At the end of the closure phase, once the reports and Remediation Plan have been agreed, the entity's Board the TI and RT providers should sign the attestation[31] to be delivered to the TTM, confirming that the test process was conducted in accordance with the requirements of this guidance and of the TIBER-EU framework.

If there was a mutual agreement to share the test results with other relevant authorities that did not participate in the test, the entity or the TCT can share the Test Summary Report and the attestation.

In order to enhance not only the tested entity's resilience, but the whole financial sector's resilience, the TCT may analyse the high-level results of all the tests to identify the key findings, thematic areas, common threats and vulnerabilities, and to disseminate these in the appropriate form to the relevant stakeholders. The TCT may also share sanitised information (e.g. lessons learned) relating to the operationalisation of the TIBER-IT with the TKC and its members. This information will allow the TKC to aggregate all the relevant information to develop a comprehensive view of the resilience of the European financial sector, and to bring about improvements where feasible. In all cases, any exchange of information should be conducted in a safe and secure manner.

The level of involvement of supervisory and oversight functions/authorities is defined by the authorities themselves and could also depend on the type of subject involved in the test. In some cases, one authority may opt to formally exclude the involvement of overseers and supervisors from the TIBER-IT testing phase, while they are primarily involved in the scoping and closure phases. In some other cases, the Authority may opt to include the overseer and supervisor throughout the entire testing process. After the completion of the test (where the overseer and supervisor have not been involved during the testing phase), the entity shall notify the finalisation of the test to its oversight and supervisory authorities, also informing the TCT; if the authorities deem it necessary, the entity shall share the Test Summary Report and the Remediation Plan with them. At this stage, overseers and supervisors may monitor the activities carried out by the entity to implement the remediation measures as envisaged in the TIBER-IT test remediation plan.

---

30 https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/shared/pdf/final_tiber-eu_guidance-for-the-tiber-eu-test-summary-report.pdf

31 The document to be signed will be provided by the TTM, based on the TIBER-EU template: https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/shared/pdf/Final_TIBER-EU_Attestation_Template_July_2020.pdf

4 Interactions and communication flows during a TIBER-IT test

During all the phases of TIBER-IT testing there are ongoing and close interactions between all the main stakeholders who cooperate towards the achievement of the common goal.

In this TIBER-IT National Guidance, all the interactions between WT and TCT/TTM have been described, as well as the close cooperation between TI and RT providers. Moreover, when deemed necessary according to the characteristics of the entity being tested, the TTM may interact with other national financial authorities and governmental security agencies as well. All parties involved in a TIBER-IT test should adopt a collaborative, transparent and flexible approach to the test. This is not valid for the BT, which should remain unaware of the test until the closing phase.

The way in which communication flows are conducted is agreed between the stakeholders, in order to protect the confidentiality of the information given. For the same reasons, the code name for the entity being tested is used throughout the test. To further protect the confidentiality of data and information, RT and TI providers may sign an NDA with the entity being tested.

Any significant deviations from the original planning should be discussed with the TTM. It is critical that all the relevant stakeholders keep each other informed at all stages to ensure that the test runs smoothly and that any issues, resource constraints and so on can be addressed in a timely fashion.

Lessons learned arising from the conduction of TIBER-IT tests may be shared by authorities in relevant national and international cyber security fora (e.g. TKC, ECRB/CIISI-EU[32], CERTFin, academic events and so on), provided that data are sanitised or given in an aggregated manner, and under no circumstances would it be possible to recognise the tested financial entity.

[32] 'Euro Cyber Resilience Board for pan-European Financial Infrastructures and Cyber Information and Intelligence Sharing Initiative'.

5 INTERACTION WITH SUPERVISORY AND OVERSIGHT FUNCTIONS/ AUTHORITIES

The TIBER-IT implementation aims to act as a catalyst for critical financial entities of the Italian financial system to enhance their cyber resilience against real potential cyber threats.

The TIBER-IT is not intended as a supervisory or oversight mandatory tool, but the role of supervisors and overseers in the process is set out in the National Guidance.

During the scoping phase, the TTM and the WT consult with the relevant supervisory and oversight authorities to verify that the business services and functions considered critical by supervisors and overseers are included in the scope of the test.

It is up to the Authorities to determine the role of the overseer and supervisor in the TIBER-IT implementation. In some cases, one Authority may opt to include the overseer and supervisor throughout the entire testing process, while in other cases, the Authority may opt for supervisory and oversight functions not to be involved in the testing phase conducted by the TI and RT providers and monitored by the WT and the TTM. The TIBER-IT-related information or documentation regarding a specific financial entity may not be shared with supervisors and overseers during the test.

After the TIBER-IT process has been completed, the entity notifies the test finalisation to the oversight and supervisory authorities, also informing the TCT; if the authorities deem it necessary, the entity shall share the Test Summary Report and the Remediation Plan with them. The tested entity should address the TIBER-IT test findings and resulting remediation activities as part of the ongoing supervisory and oversight activities.

Annexes

Annex I: TIBER-IT RACI Matrix and main deliverables

Table 1: RESPONSIBILITY ASSIGNMENT MATRIX FOR A TIBER-IT TEST

	Phase/Activity	Responsible	Accountable	Consulted	Informed	Documentation
Preparation phase	Pre-launch	TTM	TTM	WT	TCT	TIBER-IT National Guidance TIBER-EU documentation
	TI/RT services procurement	WT	Board of the entity	TTM	TI and RT Providers TCT	TIBER-EU Service Procurement Guidelines TI/RT contractual arrangements
	Pre-test risk assessment	WT	Board of the entity	TTM	TI and RT Providers	Pre-test risk assessment report
	Scoping	WT	Board of the entity	TTM Competent financial regulatory and supervisory authorities	TI and RT Providers TCT	TIBER-IT Scope Specification Document
	Launch	WT	Board of the entity	TTM	TI and RT Providers TCT	TIBER-IT Project Plan
Testing phase: threat intelligence	Provide GTL Report for financial sector	TCT	TCT	Possibly National intelligence and security agencies Other authorities, advisors and/or TI providers National and sectoral CERT/CSIRT (e.g. CERTFin)	Authorities and/or sector	GTL Report
	Targeted Threat Intelligence	TI Provider	WT	TTM RT provider Possibly national intelligence and security agencies Possibly national and sectoral CERT/CSIRT (e.g. CERTFin)	TCT	Targeted Threat Intelligence Report (TTIR)
	TI and RT Provider handover	TI Provider	WT	RT provider TTM	TCT	Targeted Threat Intelligence Report (TTIR)
Testing phase: red team test	Develop Red Team Test Plan and Attack Scenarios	RT provider	WT	WT TTM TI provider	TCT	Red Teaming Test Plan (RTTP)
	Execution of test	RT provider	WT	WT TTM TI provider	TCT	Evidence and records of Red Team Test Draft Red Team Test Report (DRTTR)
	Regular test meetings or updates	WT	Board of the entity	RT provider TTM	TCT	N/A
	Discussion as flags are captured or when leg-ups are required	RT provider	WT	WT TTM	TCT	N/A
Closure	Production of Red Team Test Report	RT provider	WT	Senior executive responsible for cyber resilience at entity	TTM TCT	Red Team Test Report (RTTR)
	Development of Blue Team Report	BT	WT	RT provider	TTM TCT	Blue Team Test Report (BTTR)
	Red/Blue Team Replay (possibly Purple Team) workshop	WT	Board of the entity	TI and RT providers BT	TTM TCT	N/A
	360° Feedback meeting	TTM	TTM	WT BT TI and RT providers	TCT	360° Feedback Report (360FR)
	Production of Test Summary Report	WT	Board of the entity	TI and RT providers TTM	TCT Competent financial regulatory and supervisory authorities Other relevant authorities	Test Summary Report (TSR)
	Remediation plan	WT	Board of the entity	TI and RT providers BT TTM	TCT Competent financial regulatory and supervisory authorities	Remediation Plan
	Signing of attestation to validate the conduct of the TIBER-IT test	Board of the entity TI and RT providers	Board of the entity	WT TTM	TCT TIBER-IT Steering Committee Other relevant authorities	TIBER-IT test attestation

ANNEX II: TIBER-IT DOCUMENTATION AND MAIN SCHEDULED MEETINGS

This document, 'TIBER-IT National Guidance v.1.0', sets out the core elements of the TIBER-IT for the Italian financial authorities, financial entities, TI and RT providers, and all the other relevant stakeholders.

For the implementation of the TIBER-IT, all the relevant stakeholders rely on a number of accompanying documents that provide additional and more specific guidance, or serve as templates for use during the testing process.

There are also certain documents to be produced by the entity, the authorities, TI/RT providers and/or other relevant stakeholders to facilitate the overall test process, as reported in Annex 11.3 of the TIBER-EU framework.

The lists of relevant documents and main meetings laid down in the TIBER-IT National Guidance are reported below. Further information can be requested at: tiber-it@bancaditalia.it.

Table 2: TIBER-IT DOCUMENTATION

	List of TIBER-IT documentation	Responsible party
1	TIBER-IT National Guidance	Financial Authorities adopting TIBER-IT
3	TIBER-IT Generic Threat Intelligence Landscape report (GTL Report)	TIBER-IT SC, TCT
4	TIBER-IT Test Project Plan	WT
5	TIBER-IT Scope specification document	WT
6	Targeted Threat Intelligence Report	TI Provider
7	Red Team Test Plan	RT Provider
8	Red Team Test Report	RT Provider
9	Blue Team Test Report	BT
10	360-degree Feedback Report	TTM, TCT
11	Test Summary Report	WT
12	Remediation Plan	WT
13	TIBER-IT Test attestation	Board of the entity, TI/RT providers

Table 3: TIBER-IT MAIN MEETINGS

	List of key formal meetings	Involved parties
1	Pre-launch meeting	TTM, WT
2	Launch meeting	TTM, WT, TI/RT providers, other relevant stakeholders
3	Scoping meeting	WT, TTM, TI/RT providers, other relevant stakeholders
4	Weekly test meetings or updates	TTM, WT, BT, TI/RT providers
5	360-degree Feedback meeting	TTM, TCT, WT, BT, TI/RT providers

Abbreviations

BT	Blue Team
CERTFin	Italian Financial Computer Emergency Response Team
CF	Critical Function
CIISI-EU	Pan-European Cyber Information and Intelligence Sharing Initiative
ECRB	Euro Cyber Resilience Board for pan-European Financial Infrastructures
GTL	Generic Threat Landscape
NDA	Non-Disclosure Agreement
PT	Purple Team
RACI	Responsibility Assignment Matrix (RACI stands for Responsible, Accountable, Consulted, Informed)
REDFin	European project - Readiness Enhancement to Defend Financial sector
RT provider	Red Team provider
TCT	TIBER Cyber Team
TIBER	Threat intelligence-based ethical red teaming
TI provider	Threat Intelligence provider
TKC	TIBER-EU Knowledge Centre
TTI	Targeted Threat Intelligence
TTM	Team Test Manager
TTPs	Tactics, Techniques and Procedures
WT	White Team
WTL	White Team Lead

Index of Figures and Tables