CONSOB
Commissione Nazionale per le Società e la Borsa

BANCA D'ITALIA
EUROSISTEMA

IVASS
Istituto per la Vigilanza sulle Assicurazioni

TIBER-IT
National Guidance

Threat Intelligence Based Ethical Red-Teaming – Italy

November 2025 - version 2.0

Francesco Trombadori, *Mattino a Ponte Fabricio*, Banca d'Italia collection

Designed and printed by the Printing and Publishing Division of Banca d'Italia

INDEX

1 Introduction 5
1.1 Foreword and regulatory framework 5
1.2 Definitions 6
1.3 Scope of application 7
1.4 What TIBER-IT is 7
1.5 Mandatory TLPT pursuant to DORA and voluntary testing 8
1.6 Legal aspects 9
2 TIBER-IT: key actors, roles, responsibilities and interactions 11
2.1 The authorities 11
2.1.1 TLPT Steering Committee for the Italian financial sector (TLPT SC) 11
2.1.2 The TIBER Authority 11
2.1.3 TIBER-IT Cyber Team (TCT) and Test Manager (TM) 12
2.2 Tested entities and service providers 12
2.2.1 Control Team (CT) and Control Team Lead (CTL) 13
2.2.2 Blue Team (BT) 13
2.2.3 Threat Intelligence Provider (TIP) 13
2.2.4 Red Team Tester (RTT) 13
3 High-level overview of the TIBER-IT process 15
3.1 Overview of the TIBER-IT process and main phases 15
3.2 Risk management during testing 16
4 Preparation phase 18
4.1 Notification 18
4.2 Initiation 18
4.3 Scoping 19
4.4 Procurement 19
5 Testing phase 20
5.1 Threat intelligence and scenario creation 20
5.2 Testing phase: *red teaming* 21
5.2.1 Attack planning (*red team test plan creation*) 21
5.2.2 Execution of the attack (*active testing*) 22
6 Closure phase 23
6.1 Report by the Red Team, the Blue Team and reproduction of the attack 23
6.2 Test summary report and remediation plan 24
6.3 Attestation 25
7 Interaction and communication flows during a TIBER-IT test 26
8 Figures index 27
9 Annexes 28
9.1 Annex I: list of acronyms 28
9.2 Annex II: additional documentation and main meetings 30

1 Introduction

1.1 Foreword and regulatory framework

The digital operational resilience of individual financial institutions and of the financial system as a whole is a priority for operators and authorities at national, European and international level. This is due to the increasing digitalization and interconnectedness of the financial system, the evolution of markets and business models, supply channels and the habits of users and customers in the use of financial services, the centrality of providers and the complexity of their supply chain. In addition, the new geopolitical context and the rise in and sophistication of cyber-attacks are important.

In this context, the strengthening of digital operational resilience benefits from the enhancement of the ability to detect, protect from and respond to cyber-attacks, both at the entity level and at the level of the financial system as a whole. This can be achieved by using advanced cybersecurity tests led by threat intelligence, i.e. Threat-Led Penetration Testing (TLPT), which were introduced into the European financial system in 2018, through the harmonized TIBER-EU[1] framework, used for testing on a voluntary basis.

At national level, Banca d'Italia, the Italian Companies and Stock Exchange Commission (CONSOB) and the Institute for the Supervision of Insurance (IVASS) collaborate to improve the overall resilience of the Italian financial system. In 2022, they jointly adopted the TIBER-IT National Guide[2] for carrying out voluntary tests, thereby implementing the EU framework. This guide was primarily addressed to critical financial entities within the Italian financial system, with the aim of enhancing its overall stability, operational efficiency and competitiveness,[3] as well as the smooth functioning, reliability and efficiency of the payment system.[4]

Regulation (EU) 2022/2554 (DORA)[5] has been applicable since January 2025. It requires mandatory TLPT[6] as a supervisory tool to verify the digital operational resilience of most important financial entities. Those for which TLPT is mandatory are identified by the competent authorities on the basis of the quantitative and quality criteria defined in the Commission Delegated Regulation (EU) 2025/1190, based on regulatory technical standards (RTS on

---

1 In 2018, the ECB published the first version of the TIBER-EU framework, a tool that mimics potential cyber-attacks by reproducing the tactics, techniques and procedures (TTPs) of real threat actors (https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html).

2 https://www.bancaditalia.it/compiti/sispaga-mercati/tiber-it/index.html.

3 See Article 5(1), Legislative Decree 385/1993 (Consolidated Law on Banking - TUB), Article 5(1), Legislative Decree 58/1998 (Consolidated Law on Finance - TUF) and Article 3(1), Legislative Decree 209/2005 (Italian Private Insurance Code - CAP).

4 See Article 146(1) of the TUB.

5 The current version of the text is available on the EurLex website (https://eur-lex.europa.eu/eli/reg/2022/2554/oj). Any future updates, resulting from subsequent amendments or corrections, will likewise be accessible on the EurLex website, under the 'Consolidated texts' section (https://eur-lex.europa.eu/collection/eu-law/consleg.html).

6 See Articles 26, which regulates the 'Advanced testing of ICT tools, systems and processes based on TLPT', and 27, which establishes the 'Requirements for testers for carrying out TLPT'.

TLPT) and developed in accordance with the TIBER-EU.[7] In this regard, the TIBER-EU framework was recently updated to bring it into line with the changes introduced by DORA.[8]

At national level, the compliance with DORA was implemented by Legislative Decree 23/2025.[9] It designates Banca d'Italia, CONSOB and IVASS as the competent authorities 'for compliance with the obligations laid down by the same Regulation for the supervised entities by the same authorities, according to their respective supervisory mandates'.[10] These attributions also apply to TLPT.[11] For significant banks, the competent authority is the European Central Bank (ECB).

In this context, the TIBER-IT National Guide (the 'Guide') has been integrated and updated to take account of the DORA, the RTS on TLPT, the new version of the TIBER-EU framework, and the national provisions.

The Guide offers a methodology and an operative model for both voluntary and mandatory TLPT tests; the latter are carried out by the financial entities identified by Banca d'Italia, CONSOB and IVASS, according to their respective powers.

1.2 Definitions

Throughout the rest of the document, unless otherwise specified:

- 'the authorities' shall mean Banca d'Italia, CONSOB and IVASS;
- 'Competent authority' means the authority pursuant to Article 46 of DORA;
- 'TIBER Authority' is the competent authority that carries out activities relating to a TIBER-IT test or the authority delegated to do so pursuant to Article 26(10) of DORA on the basis of national agreements between the authorities. If the TIBER-IT test is carried out pursuant to DORA, the TIBER Authority is considered to be the 'TLPT Authority', as defined in the RTS on TLPT (see §2.1.2);
- 'financial entities' include:

---

7 The current version of the text is available on the EurLex website (https://eur-lex.europa.eu/eli/reg_del/2025/1190/oj). Any future updates, resulting from subsequent amendments or corrections, will likewise be accessible on the EurLex website, under the 'Consolidated texts' section (https://eur-lex.europa.eu/collection/eu-law/consleg.html). In this document, the reference to RTS on TLPT shall be understood as referring to the text of the aforementioned Delegated Regulation.

8 https://www.ecb.europa.eu/press/intro/news/html/ecb.mipnews250211.en.html.

9 Legislative Decree 23/2025, Measures for the alignment of national legislation with the provisions of the Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011, and for the transposition of Directive (EU) 2022/2556 of the European Parliament and of the Council of 14 December 2022 amending Directives 2009/65/EC, 2009/138/EC, 2011/61/EU, 2013/36/EU, 2014/59/EU, 2014/65/EU, (EU) 2015/2366 and (EU) 2016/2341 as regards digital operational resilience for the financial sector.

10 Author's translation. See Article 3.

11 Italy did not exercise the option provided for in Article 26 of DORA to designate a single public authority in the financial sector that is responsible for TLPT-related matters at national level.

i. financial entities as defined in Article 2(2) of DORA, under the competence of the authorities;

ii. payment systems;

iii. supporting technological or network infrastructures;12

iv. Poste Italiane S.p.A., for the activities of Bancoposta, as referred to in the Presidential Decree 144/2001;13

v. financial intermediaries pursuant to Article 106 of the TUB;

- 'financial sector' refers to the financial entities mentioned above.

1.3 Scope of application

The Guide is addressed to financial entities, both for mandatory TLPT pursuant to DORA and for voluntary tests, their ICT third-party service providers (if they are included in the scope of the test), threat intelligence service providers (threat intelligence - TI), and red team testers (RTT).

However, other financial entities and/or other types of entity[14] can also communicate their interest in conducting a voluntary test at the single point of contact for each request for TIBER-IT-related information, using the following e-mail address: tiber-it@bancaditalia.it. In this case, the proposal will be reviewed, and its appropriateness will be assessed in light of improving the overall resilience of the financial sector by considering, for example, the entity interconnections with other financial entities, their cyber maturity, and the resources available to the authorities to oversee the test.

The Guide does not apply to mandatory TLPTs under DORA for significant banks, for which reference is made to what is established by the Single Supervisory Mechanism (SSM), while it remains valid for voluntary tests.

1.4 What TIBER-IT is

TIBER-IT is the national contextualization of the TIBER-EU framework and takes account of national specificities. The provisions contained in TIBER-IT aim to ensure mutual recognition of the tests by other jurisdictions transposing the TIBER-EU, and to provide further practical guidance for TLPT pursuant to DORA.

By conducting the TIBER-IT test, financial entities can improve their operational resilience, and the authorities can obtain adequate insurance regarding cyber resilience at both individual and sectoral levels, for the purposes of financial stability as well.

---

12 The term '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 Regulation of 9 November 2021 issued by Banca d'Italia).

13 The application of some DORA articles to Bancoposta was provided for by Legislative Decree 23/2025.

14 For example, entities involved in activities that are relevant to the financial system.

Throughout the process, the TIBER-IT tests require all the relevant stakeholders (multi-stakeholder approach) to be heavily involved. The entities identify the main stakeholders to be involved in their test. Since TLPT is an intrusive tool and the test has to be conducted in the production environment, all the parties involved, the corporate management, and the Control Team in particular (CT, see §2.2.1) shall give the highest priority to clearly defining the test scope, identifying the critical functions (CFs)[15] to be included in the test, and applying effective risk management controls throughout the process.

In this context, Banca d'Italia is the lead authority of TIBER-IT and carries out its tasks in close cooperation with CONSOB and IVASS.

The maintenance of TIBER-IT and its alignment with TIBER-EU, DORA and other international best practices are led by an inter-institutional coordination group among the three authorities (the TLPT Steering Committee, see §2.1.1).

1.5 Mandatory TLPT pursuant to DORA and voluntary testing

DORA (Articles 26 and 27) requires financial entities identified as critical or having a potentially systemic impact to carry out Threat-Led Penetration Testing (TLPT). As previously stated, such entities are designated in Italy by the respective competent authorities – namely Banca d'Italia, CONSOB, and IVASS – based on their respective statutory mandates. For banks classified as significant, the competent authority is the ECB.

The methodology for conducting a TLPT pursuant to DORA, detailed in the RTS on TLPT, was developed in accordance with the TIBER-EU framework. Both TIBER-EU and TIBER-IT, its national implementation as referred to in this Guide, can therefore be seen to be compliant with the TLPT requirements of DORA, while also providing further operational guidance.[16]

DORA and the RTS on TLPT establish the regulatory framework and set out the normative requirements governing TLPT, while TIBER-EU and TIBER-IT provide methodological support on how a TLPT should be carried out both by the tested entity and by the authorities.

Considering the alignment between TIBER-EU and the TLPT pursuant to DORA, TIBER-IT is the reference model for TLPT to be carried out pursuant to DORA for the financial entities (properly) identified by the competent authorities.

In the case of TLPT carried out pursuant to DORA, the competent authority identifies the financial entity mandated to carry out the tests by formally

---

15 Throughout the rest of the document, the terms 'critical function' or 'critical or important function' are interchangeable. DORA (Article 3, no. 22) defines a critical or important function as: 'a function, the disruption of which would materially impair the financial performance of a financial entity, or the soundness or continuity of its services and activities, or the discontinued, defective or failed performance of that function would materially impair the continuing compliance of a financial entity with the conditions and obligations of its authorisation, or with its other obligations under applicable financial services law'.

16 See also the ECB's publication in September 2024: 'Adopting TIBER-EU will help devise DORA requirements', https://www.ecb.europa.eu/press/intro/publications/pdf/ecb.miptopical240926.en.pdf.

communicating it.[17] The TIBER Authority will then notify the financial entity of the start of the test (see §4.1).

Financial entities not mandated to perform TLPT can show interest in voluntarily participating in a TIBER-IT test by notifying the single contact point (see §1.3). In such a case, the decision to participate in the test should be taken at the level of the board of directors, or similar body of the financial entity or a delegate.

The differences between a TLPT pursuant to DORA and a voluntary test lie, broadly speaking, in the former being mandatory and also used as a supervisory tool. The process of conducting the individual test is the same and the main goal is to increase the cyber resilience of the tested entity, including by leveraging the learning opportunities experienced during the test.

To this end, in addition to what is included in this Guide in the following chapters, based on the TIBER-EU framework and accompanying documents,[18] tested entities must adhere to the applicable version of DORA and to the RTS on TLPT in effect at the time of testing.

In accordance with the TIBER-EU framework and the provisions contained in DORA, cross-border testing and/or TLPT that involve more than one financial entity will be possible, especially in the case of entities providing services in several countries and/or sharing the same technology infrastructure or the same ICT third-party service providers: namely the multiparty testing,[19] which includes joint tests and pooled tests.[20]

1.6 Legal aspects

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

Consulting the TIBER-EU framework in addition to this Guide is recommended, as the two are complementary: the TIBER-IT National Guide does not provide an in-depth description of all the concepts and processes derived from the TIBER-EU framework, which are instead comprehensively presented therein.

For any aspects not expressly covered by this Guide, reference shall be made to the provisions set out in DORA, in the RTS on TLPT, in the TIBER-EU framework and in the related supporting documents. All references and cross-references contained in this Guide shall be deemed to refer to the version in force at the time of the test. Any subsequent updates to the TIBER-EU framework and to the RTS on TLPT shall automatically be applicable by virtue of the references contained in this Guide.

---

17 Details of the identification process are not included in this Guide.

18 See §9.2. The supplementary documentation is updated and published by the ECB on its institutional website.

19 See also Section 3.10 of the TIBER-EU framework.

20 See Article 1.18 of the RTS on TLPT (joint TLPT) and Article 26.4 of DORA.

Each participant in a TIBER-IT test is the only and exclusive entity responsible for performing the activities assigned to it by this Guide, including compliance with the applicable laws and regulations.

Tested entities remain fully responsible at any time for the risks associated with conducting the test and for any negative impact on their services and third parties.

This Guide transposes the TIBER-EU framework.

2 TIBER-IT: KEY ACTORS, ROLES, RESPONSIBILITIES AND INTERACTIONS

The following describes the main actors, roles, responsibilities and interactions between the stakeholders involved in the activities for the management and implementation of TIBER-IT and in the single test.[21]

With regard to the single test, the main stakeholders are informed about their respective roles and responsibilities. It shall be ensured that:

- the test is conducted in a controlled manner using a risk-based approach;
- a clear protocol is established for all the concerned parties that sets out the information flows throughout the test and how information can be stored and shared.

2.1 THE AUTHORITIES

The authorities play a role both in the implementation and review of the TIBER-IT methodology and in the oversight of the execution process for individual tests:

- through participation in the TLPT Steering Committee for the Italian financial sector (TLPT SC);
- in their capacity as the TIBER Authorities;
- by establishing the TIBER Cyber Team (TCT)[22] and appointing the Test Manager (TM).

2.1.1 TLPT STEERING COMMITTEE FOR THE ITALIAN FINANCIAL SECTOR (TLPT SC)

To ensure coordination among the authorities, and the maintenance and implementation of the TIBER-IT, Banca d'Italia, CONSOB and IVASS have a high-level committee, called the TLPT Steering Committee for the Italian financial sector (TLPT SC), following on from the previous TIBER-IT Steering Committee, established following the adoption of the TIBER-IT National Guide in 2022.

2.1.2 THE TIBER AUTHORITY

The TIBER Authority:

- is one of the authorities that adopted TIBER-IT and carries out specific activities as part of a TIBER test;
- if the test is carried out pursuant to DORA, it is considered as the related 'TLPT Authority';[23]

---

21 Throughout the rest of the document, reference is made without distinction to the terms 'test', 'TIBER-IT test', and 'TLPT', given that the test process is basically the same.

22 In this Guide, reference is made without distinction to the terms 'TIBER Cyber Team' and 'TLPT Cyber Team'.

23 Article 1(7) of the RTS on TLPT defines 'the TLPT Authority' as: '(a)[...] (b) the authority in the financial sector to which the exercise of some or all of the tasks in relation to TLPT is delegated in accordance with Article 26(10) of Regulation (EU) 2022/2554; (c) any of the competent authorities referred to in Article 46 of Regulation (EU) 2022/2554'

- in the event that the delegation provided for under Article 26, paragraph 10 of DORA is exercised, it coincides with the delegated authority.

For multiparty testing, there might be more than one TIBER Authority, including from other countries.

The TIBER Authorities promote the execution of TIBER-IT tests by financial entities, steer their annual and multi-annual planning and provide guidance and methodological support for the conduct of the test.

For the coordinated tasks assigned to the TIBER Authorities, a TIBER-IT Cyber Team (see §2.1.3) has been set up.

2.1.3 TIBER-IT Cyber Team (TCT) and Test Manager (TM)

The TIBER-IT Cyber Team (TCT) comprises representatives from the authorities adopting this Guide and is supported by a stable pool of resources guaranteed by Banca d'Italia.

The TCT liaises with other authorities and/or countries and with the TIBER Knowledge Centre (TKC) on an ongoing basis.[24] The role of the TCT is further outlined in Section 3.2 of the TIBER-EU framework.

For each test, a Test Manager (TM) is appointed, normally from among the staff composing the TCT, assisted by one or more substitutes. The main task of the TM is to oversee the execution of the test by the tested entity and to continuously check that the tested entity conducts the test in a controlled manner and in accordance with this Guide and the TIBER-EU framework. The TM is not responsible for the actions of the Control Team, for the execution of the test, for its results or for the Remediation Plan.

For additional information regarding the role of the TM, refer to Section 3.3 of the TIBER-EU framework and to all the phases of the process.

2.2 Tested entities and service providers

In the context of a single test, the key actors involved are:

- the Control Team (CT) and the Control Team Lead (CTL) of the tested entity;
- the Blue Team (BT) of the tested entity;
- the Threat Intelligence Provider (TIP);
- the Red Team Tester (RTT), which can be an external provider or dedicated personnel at the tested entity.

[24] The TKC was established at the ECB and is a forum composed of representatives of the institutions implementing the TIBER-EU framework. Its main objectives are to: i) maintain the TIBER-EU framework; ii) facilitate knowledge transfer and foster collaboration across jurisdictions; iii) support institutions in their national implementations and provide a centralized repository for the relevant documents; and iv) monitor national implementations to ensure mutual recognition of TIBER tests.

2.2.1 Control Team (CT) and Control Team Lead (CTL)

For each test, the tested entity sets up a Control Team (CT), led by a Control Team Lead (CTL). The CTL plays a key role in the proper conduct of the test and an alternate is therefore also usually appointed. The CTL is responsible, among other things, for the definition of the scope of the test and its overall execution.

For additional information regarding the role of the CT and the CTL, refer to Section 3.4 of the TIBER-EU framework and to the sections covering all phases of the process. Further details on the roles, responsibilities and composition of the CT are provided in the TIBER-EU Control Team Guidance document.

2.2.2 Blue Team (BT)

For each test, the Blue Team (BT) is composed of all the other staff (not included in the CT) of the tested entity, including third parties, especially those who manage and run the ICT systems (and the people, processes and technologies) of the tested entity.

Specifically, the BT also includes the staff responsible for defending the tested entity's network and information systems. It is crucial for the BT to remain unaware of the test when it is carried out and to be completely excluded from the preparation and execution of the test.

The role of the BT is further outlined in Section 3.5 of the TIBER-EU framework.

2.2.3 Threat Intelligence Provider (TIP)

The Threat Intelligence Provider (TIP) is an external provider whose threat analysis services have been procured by the CT in line with the standards and minimum requirements set out in the TIBER-EU Guidance for Service Provider Procurement document. The TIP gathers targeted information about the tested entity, emulating the research that would be done by an expert attacker and developing entity-specific threat scenarios. The TIP should use multiple intelligence sources to provide the most accurate and up-to-date assessment possible.

The role of the TIP is further outlined in Section 3.6 and Chapter 7 of the TIBER-EU framework.

2.2.4 Red Team Tester (RTT)

The Red Team Tester (RTT) plans, develops and executes attack scenarios on the people, processes, systems and services included in the scope of the test. Its purpose is to try to breach the tested entity's security measures, following a methodology of rigorous and ethical red teaming and always within the boundaries of this Guide and the TIBER-EU framework. The rules of engagement and the specific requirements for testing are laid down by the RTT and the tested entity.

The role of the RTT is further outlined in Section 3.6 and Chapters 8 and 9 of the TIBER-EU framework.

The RTT is generally an external provider, owing to the possible contribution of a more independent perspective than that of internal staff and the possibility to have more resources and up-to-date expertise. If this is the case, the services were procured by the CT in line with the standards and minimum requirements set out in the TIBER-EU Guidance for Service Provider Procurement document. In agreement with the TM, the RTT can be internal to the tested entity and must meet the same standards and requirements as the external RTT, in addition to what is set out in Section 3.6.3 of the TIBER-EU framework.

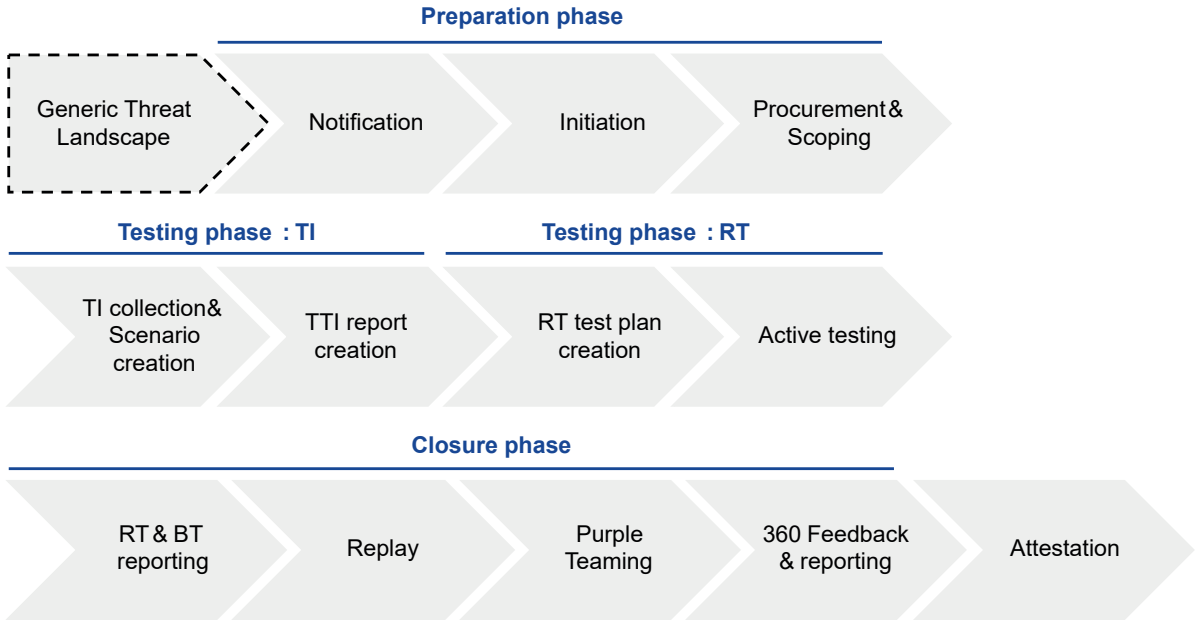
3 High-level overview of the TIBER-IT process

This section describes the main milestones and the documentation of the various phases of the testing process. For a comprehensive and detailed description of what is included in each phase of the process, the documentation to be produced as well as the meetings to be held, reference should be made to the TIBER-EU framework and its supporting documents and, in the case of mandatory TLPT pursuant to DORA, to the RTS on TLPT.

3.1 Overview of the TIBER-IT process and main phases

The overall process for a TIBER-IT test consists of three main phases:[25] i) preparation, ii) testing, and iii) closure. This process is fully aligned with the one described in the TIBER-EU framework (Figure 1).

Figure 1: OVERVIEW OF THE PROCESS – MAIN PHASES AND ACTIVITIES (SOURCE: ECB)



The *preparation* phase starts with a *notification* from the TIBER Authority that officially marks the start of the test, through a communication sent to the contact point designated by the tested entity (i.e. *written notification*). The tested entity, through the CT, then produces the documents and information preliminary to the start of the project (*initiation*), identifies the perimeter of the test and its objectives (*scoping*), acquires the external services (*procurement*) for threat intelligence and, if necessary, red teaming. The preparation phase is completed no later than six months after receiving the written notification.

[25] The definition and provision of a Generic Threat Landscape (GTL) by the TIBER Authority for the Italian financial sector is optional.

The *testing* phase starts with the analysis of the threat landscape (*threat intelligence*) by the TIP, followed by the definition of targeted threat scenarios (*TI collection & scenario creation*). Within a period of between 4 and 6 weeks, the TIP finalizes the *Targeted Threat Intelligence Report* (TTIR). The testing phase then enters the testing period (i.e. *red teaming*), during which the RTT, indicatively within the first 2 or 3 weeks, develops a detailed plan to simulate an attack (*RT test plan creation*), followed by *active testing* for at least 12 weeks.

At the closing phase (i.e. *closure*), the tested entity and the RTT produce, under their remit, the final reports on the project: the *Red Team Test Report* (RTTR), within four weeks after the closure of the testing phase; the *Blue Team Test Report* (BTTR), within ten weeks of the closure of the testing phase; the *Test Summary Report* (TSR) and the *Remediation Plan* (RP) within eight weeks of the approval of the previous reports. Moreover, within ten weeks of the end of the testing phase, the BT and the RTT cooperate in the *Purple Teaming* phase (PT).

The documentation prepared by the various actors during the conduct of the TIBER-IT test is primarily based on the TIBER-EU templates, although it can be customized if necessary by the TIBER Authority to take account of national specificities. The documentation is available on the ECB's website[26] and on Banca d'Italia's website in the section dedicated to TIBER-IT.[27]

Several formal meetings between those involved in the test are planned at various phases of the process. Under the agreement between the TM and the CTL, some of these meetings may be held jointly; in addition, further meetings may be scheduled with a more operational focus or as opportunities for discussion.

Where not explicitly specified, the detailed procedures for the submission of the required documentation by the tested entity at each phase of the process will be communicated by the TM on a case-by-case basis.

3.2 Risk management during testing

The test is carried out on the people, systems and services that support the critical functions of the tested entity in the production and live environment. Given that the execution of the test carries potential risks, the CT must implement appropriate controls to ensure that the test does not compromise the proper functioning of the tested entity, its customers, or impact overall financial stability. The tested entity is fully responsible for the test itself.

For these reasons, the CT shall carry out an appropriate assessment of the specific risks associated with the test and may interrupt the test at any time, notifying the TM, if it deems that its continuation poses an unacceptable risk to the tested entity. The risk analysis and the relative management plan shall be continuously updated in response to changes in the scenario or any other element that may alter the risk profile associated with the ongoing activity.

---

26 See https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html.

27 The TIBER-IT page is accessible on Banca d'Italia's website at: Home/Our Role/Market and Payment System Oversight/TIBER-IT: https://www.bancaditalia.it/compiti/sispaga-mercati/tiber-it/index.html.

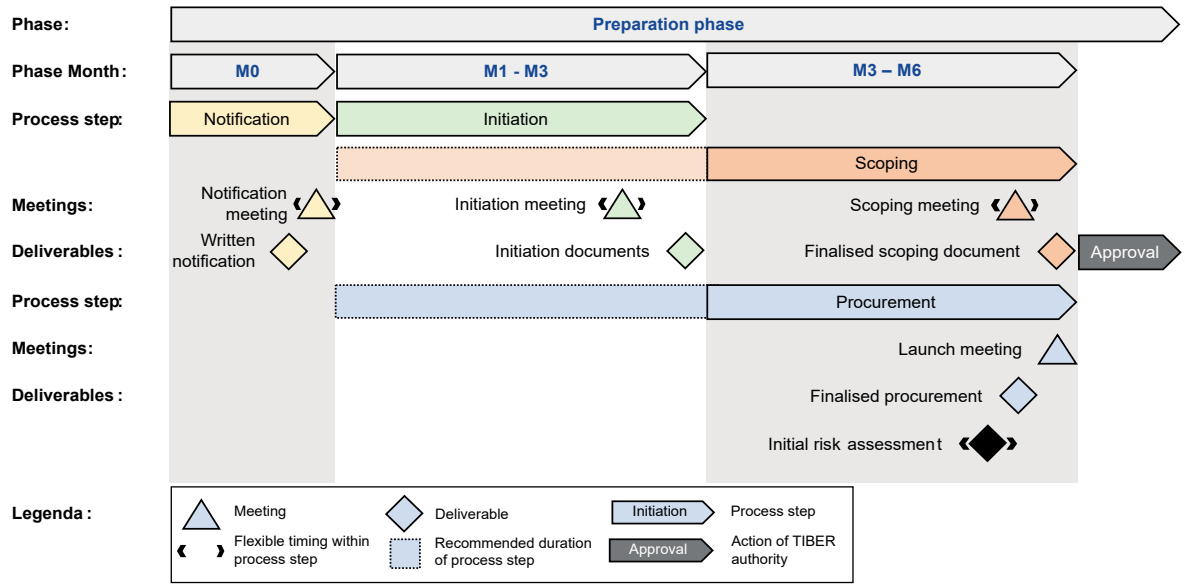
The functions and ICT systems involved in the test typically contain information protected by law, such as confidential banking data, electronic communications, and personal data. Full compliance with applicable legislation must therefore be ensured throughout the duration of the test, along with the integrity, availability, and confidentiality of such information, through the adoption of appropriate risk management measures.

For additional information regarding the risk management, refer to Chapter 4 of the TIBER-EU framework.

4 PREPARATION PHASE

The *preparation* phase consists of four steps (Figure 2): 1) notification, 2) initiation, 3) identification of the perimeter of the test (*scoping*), and 4) acquisition of services (*procurement*).

Figure 2: OVERVIEW OF THE PREPARATION PHASE (SOURCE: ECB)



Some of these activities can be conducted in parallel or started prior to notification (e.g. the acquisition of services).

Each preparation phase activity is briefly described in this Guide. For further details, refer to the provisions of the TIBER-EU framework, particularly Chapter 6.

4.1 NOTIFICATION

The TIBER Authority sends a communication (*written notification*) to the designated contact point of the tested entity. This notification marks the beginning of the *preparation* phase, which may last up to six months, as well as the start of the test itself.

Following the notification, the TM arranges a meeting (*notification meeting*) with the tested entity to present the main features of the test, with a particular focus on roles, responsibilities and testing procedures.

4.2 INITIATION

In the *initiation* step, the tested entity drafts the initial documents necessary for the launch of the test (*Initiation Documents* - IDs), which must include, among other things: i) high-level project planning; ii) the code name for the test; iii) the communication channels to be used; iv) the CTL's contact details; and v) high-level information on the CFs supported by third parties and/or provided to or by other jurisdictions.

The initiation documents are submitted to the TM and presented by the CTL during the *initiation meeting*, which takes place within three months of receipt of the initial notification.

For further details on the content of initiation documents, refer to the TIBER-EU Initiation Documents Guidance.

4.3 Scoping

During this phase, the tested entity identifies the perimeter of the test, in terms of CFs, including the people, systems and services supporting them. In line with operational risk management practices, the tested entity may conduct or rely on a Business Impact Analysis (BIA) to determine the CFs to be tested.

The objectives (*flags*) to be achieved are also defined during this phase. These flags may, however, be modified iteratively throughout the test, based on the TI output, the evolution of the test itself, and in agreement with the TM; in such cases, the risk assessment plan (see §3.2) should also be updated.

The outcome of this activity is the drafting of the *Scope Specification Document* (SSD), which is discussed with the TM during a dedicated meeting (*scoping meeting*), together with the presentation of risk mitigation measures and the related documentation.

The TM consults the competent authority to verify that business services and functions deemed critical and/or of particular interest by the competent authority are included within the scope of the test, and to gather any observations regarding the defined flags to be achieved.

Within six months of the initial notification, the finalized SSD document, approved by the Board of Directors of the tested entity,[28] is submitted to the TM for validation by the TIBER Authority.

For further details on the content of the SSD, refer to the TIBER-EU Scope Specification Document Guidance.

4.4 Procurement

Considering the level of risk associated with testing in the production and live environment, as well as the sensitive data managed by tested entities, it is essential that both the TIP and the RTT possess the highest levels of expertise, capabilities and qualifications. Accordingly, the tested entity, by means of the CT, is responsible for selecting – via a rigorous due diligence process – an external TIP and an RTT (internal or external), verifying their suitability in accordance with the TIBER-EU Guidance for Service Provider Procurement, and providing supporting evidence to the TM.

---

28 Or by another formally appointed committee or personnel member with responsibilities for activities relating to testing and for liaising with the authorities.

5 TESTING PHASE

The *testing* phase begins following the approval of the SSD, once the TIP and the RTT have been appointed and all the activities in the preparation phase have been completed. This phase consists of two sub-phases: *threat intelligence* and *red teaming*.

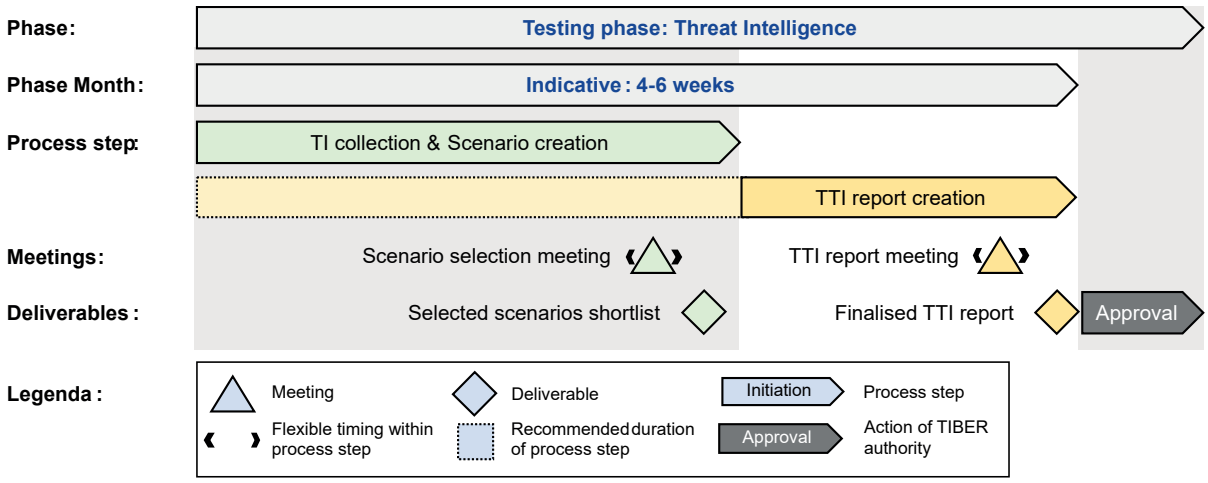
This Guide provides a brief description of each sub-phase. For further details, refer to the provisions of the TIBER-EU framework, particularly Chapters 7 and 8.

Under no circumstances can the TIP or the RTT use, in any other context outside the test, any information on the risks, threats and vulnerabilities identified, whether individually or in aggregate form.

5.1 THREAT INTELLIGENCE AND SCENARIO CREATION

The *threat intelligence* sub-phase is carried out by the TIP and lasts between 4 and 6 weeks in total (Figure 3). Based on the analysis of the cyber-threat landscape in which the tested entity – potentially using one or more GTL Reports – and on the detailed information collected on the tested entity (*TI collection*), the TIP[29] draws up various cyber-attack scenarios involving real threat actors (*scenario creation*), tailored to the tested entity and the identified CFs. These scenarios are presented during a dedicated meeting (*scenario selection meeting*).

Figure 3: OVERVIEW OF THE TESTING PHASE – THREAT INTELLIGENCE (SOURCE: ECB)



The TIP then prepares a document summarizing the analysis performed, the related findings, the scenarios proposed, and those selected (TTIR). For further

[29] The TIP must always display deeply ethical behaviour and the TTI activities must always be conducted in compliance with the applicable laws.

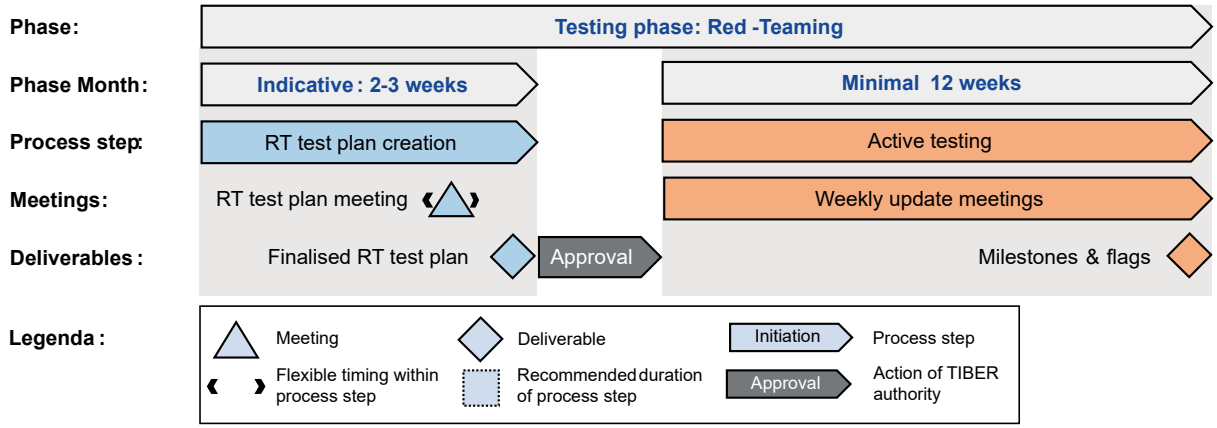
details on the content of the TTIR, refer to the TIBER-EU Targeted Threat Intelligence Report Guidance.

The TTIR is discussed with the CT and the TM during a dedicated meeting (*TTI report meeting*) and then submitted via the CT for approval of the TM, who verifies the document's compliance with the requirements set out in the TIBER-EU framework.

5.2 TESTING PHASE: *RED TEAMING*

The testing phase continues with the *red teaming* sub-phase, which is further split into two activities (Figure 4): i) development of the test plan (*red team test plan creation*) and ii) execution of the attack (*active testing*).

Figure 4: OVERVIEW OF THE TESTING PHASE – RED TEAMING (SOURCE: ECB)



5.2.1 ATTACK PLANNING (*RED TEAM TEST PLAN CREATION*)

This activity, which typically lasts between 2 and 3 weeks, involves the RTT detailing the previously selected attack scenarios and defining a plan for each one, including, among other things: the timeline, sequence of actions to be simulated (*kill chain*), the TTPs to be used, the flags to be achieved, and any leg-ups[30] that may be requested. The RTT presents the overall plan (RTTP) to the CT and the TM, which must also include guidance on risk management, during a dedicated meeting (*RT test plan meeting*). For further details, refer to the provisions of the TIBER-EU framework, particularly Section 8.3 and for the content of the RTTP, refer to the TIBER-EU Red Team Test Plan Guidance.

Once finalized, the RTTP is approved first by the CT and then by the TM, who verifies the document's compliance with the requirements set out in the TIBER-EU framework.

30 These consist of additional information and/or direct access to the systems and the network, e.g. by using ad hoc credentials, which the CT can provide to the RTT.

5.2.2 Execution of the attack (*active testing*)

This task must give the RTT[31] sufficient time to carry out a realistic and comprehensive test in which all the attack phases are executed and, where possible, all the test objectives are achieved. The duration allocated to the test should be proportionate to the scope, the tested entity's resources, and the attack scenarios defined in the RTTP. In any case, the active testing phase must last at least 12 weeks.

The RTT may deviate from the attack scenarios outlined in the RTTP, as the activity requires creativity – like real-world cyber-attacks – especially when facing obstacles or in order to develop alternative approaches to achieve the test objectives.

During the attack, the RTT may be unable to proceed to subsequent steps due to time constraints or because the BT has successfully protected the tested entity. In such cases, the CT and the TM may agree to provide some help to allow the test to continue (i.e. a *leg-up*). Experience shows a direct correlation between the relevance of the additional information that the CT provides to the RTT and the overall benefit that the tested entity derives from the test. Each leg-up provided must be duly documented and included in the *Red Team Test Report*.

Throughout the testing phase, the CT and the RTT ensure regular monitoring of the test's progress, for example by means of daily communications and/or meetings via agreed channels, to report important updates such as the achievement of a flag, the identification of potentially critical vulnerabilities, security issues, or other events that could jeopardize the continuation of the test (or parts thereof) or the confidentiality, integrity and availability of the corporate systems. Additionally, both the CT and the RTT provide updates to the TM at least weekly (*weekly meeting*).

If RTT activities are detected by the BT, and the CT is unable to maintain the confidentiality of the test (or of the individual scenario), the test may continue in *Purple Teaming (*PT) mode, subject to agreement with the TM.

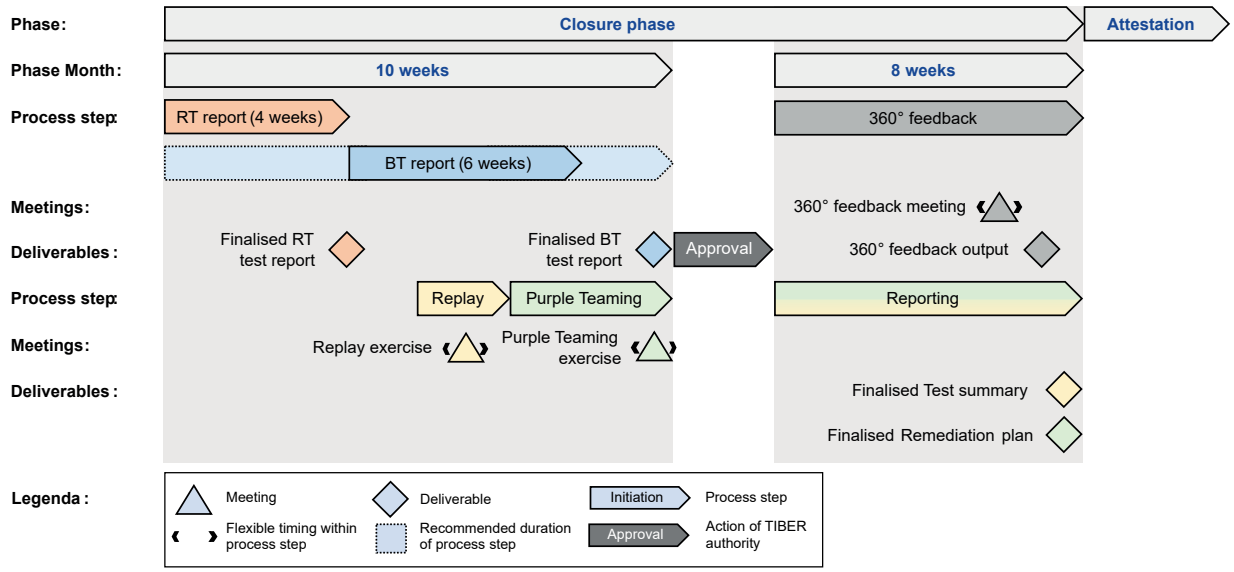
For further details, refer to the provisions of the TIBER-EU framework, particularly Section 8.4 and for more information on the PT, refer to the TIBER-EU Purple Teaming Guidance.

[31] The RTT should always display deeply ethical behaviour, and activities must always be carried out in accordance with the applicable laws.

6 CLOSURE PHASE

The *closure* phase begins upon completion of the attack execution and is dedicated to the analysis of the activities carried out during the test, together with the BT, which by then has been informed about the test, and to planning the necessary improvements to strengthen the cyber resilience of the tested entity (Figure 5).

Figure 5: OVERVIEW OF THE CLOSURE PHASE (SOURCE: ECB)



The test ends with the issuance of the attestation. Any subsequent monitoring of the remediation plan falls under the responsibility of the competent authority, as part of its ordinary supervisory activities.

For further details, refer to the provisions of the TIBER-EU framework, particularly Chapter 9.

6.1 REPORT BY THE RED TEAM, THE BLUE TEAM AND REPRODUCTION OF THE ATTACK

The first step of the closure phase, which lasts no more than ten weeks, includes several technical activities that report and reproduce the test:

- drafting of the *Red Team Test Report*;
- drafting of the *Blue Team Test Report*;
- execution of the *Replay exercise;*
- carrying out the *Purple Teaming*.

Within four weeks of the end of the attack phase, the RTT submits a document (RTTR) to the CT and the TM that provides a detailed summary of all the activities carried out during the attack, including the timeline, the flags achieved, TTPs

used successfully, the vulnerabilities identified, the root causes, and the related recommendations for remediation.

For further details on the content of the RTTR, refer to the TIBER-EU Red Team Test Report Guidance.

The BT uses the RTTR, including a draft version if necessary, to prepare a document (BTTR) containing details of the activities performed or not performed by the BT during the attack phase in response to RT's actions (e.g. log and alert analysis, containment and mitigation measures, etc.). The BTTR is finalized and submitted to the CT and the TM within ten weeks of the end of the attack phase.

For further details on the content of the BTTR, refer to the TIBER-EU Blue Team Test Report Guidance.

The BTTR, including a draft version if applicable, is used together with the RTTR during the replay exercise, in which the RTT and the BT jointly revisit the executed attack scenarios, following the chronological sequence of the key activities carried out by each team, with the aim of conducting a technical review of the actions taken and the countermeasures applied or considered. Finally, the RTT and the BT also cooperate on a PT exercise, in which additional activities that could have been carried out by the RTT – but were not due to time constraints or excessive risk – and/or TTPs that could have been used during the test are analysed.

For further details on the PT exercise, refer to the TIBER-EU Purple Teaming Guidance.

6.2 Test summary report and remediation plan

In the second step of the closure phase, once the RTTR and BTTR have been finalized, the tested entity prepares a summary document (TSR) outlining the overall testing process and its outcomes, based on all the documentation produced during the test.

For further details on the content of the TSR, refer to the TIBER-EU Test Summary Report Guidance.

In parallel, based on the recommendations provided by the RTT and the BT, the tested entity prepares a remediation plan (RP) aimed at addressing the vulnerabilities (and their underlying causes) identified during the test. The RP is not limited to purely technical remediation actions but, where necessary, includes broader measures designed to improve the tested entity's internal processes.

For further details on the content of the RP, refer to the TIBER-EU Remediation Plan Guidance.

The TM consults the competent authority for any observations regarding the TSR and the RP drafted by the tested entity.

Within eight weeks of the finalization of the RTTR and BTTR, the tested entity submits the final versions of the TSR and RP to the TM; the RTTR is also submitted to the competent authority, if it is different from the TIBER Authority.

Prior to the formal conclusion of the test, the TM arranges a meeting to collect feedback from all the parties involved in the testing process (*360-degree Feedback Meeting*), with the aim of jointly reviewing the test and identifying potential improvements in the approach taken, for future tests, and for the TIBER-IT methodology as a whole.

6.3 Attestation

At the end of the closure phase, once the TIBER Authority has assessed compliance with the applicable requirements for the overall testing process and approved both the TSR and RP, an *attestation*[32] is issued to the tested entity confirming that the testing process has been completed and conducted in accordance with the requirements set out in this Guide and, in the case of mandatory TLPT pursuant to DORA, with the provisions of DORA and the RTS on TLPT. The TIBER Authority does not provide any assessment of the outcomes of the test, which by its very nature is not a 'pass or fail' exercise.

The attestation may be used by the tested entity for potential mutual recognition of the test by other national authorities or jurisdictions.

For further details on the content of the attestation refer to the TIBER-EU Attestation Guidance.

[32] Subject to any agreements between the competent authorities regarding the responsibility for issuing and communicating the attestation in cases where the delegation procedures provided for under DORA are applied.

7 INTERACTION AND COMMUNICATION FLOWS DURING A TIBER-IT TEST

Continuous and close interaction among all key stakeholders is ensured throughout the TIBER-IT testing phases.

This Guide outlines all interactions between the CT and the TCT/TM, as well as the close cooperation between the TIP and the RTT. Furthermore, where deemed necessary and depending on the characteristics of the tested entity, the TM may also engage with other national and international financial authorities and governmental cybersecurity agencies.

All parties involved in a TIBER-IT test adopt a collaborative, transparent and flexible approach to the testing process. This does not apply to the BT, which must remain unaware of the test until the closure phase.

The communications methods are agreed upon by the relevant parties to safeguard the confidentiality of the information exchanged. For the same reason, the code name of the tested entity is used throughout the duration of the test. To further protect the confidentiality of data and information, the TIP and RTT should sign a Non-Disclosure Agreement (NDA) where appropriate with the tested entity.

Any significant deviations from the initial planning are discussed with the TM. It is essential that all stakeholders remain informed at every stage to ensure that the test proceeds without disruption and that any issues (e.g. resource constraints or logistical and operational difficulties) can be addressed in a timely manner.

In order to enhance not only the resilience of the tested entity but also that of the financial sector as a whole, the TCT may analyse the high-level results from all tests (e.g. the *Test Summary Report*) to identify key issues, thematic areas, common threats and vulnerabilities, and disseminate them in anonymized form to the relevant stakeholders.

8 Figures index

Figure 1: Overview of the process – main phases and activities (source: ECB) 15

Figure 2: Overview of the preparation phase (source: ECB) 18

Figure 3: Overview of the testing phase – threat intelligence (source: ECB) 20

Figure 4: Overview of the testing phase – red teaming (source: ECB) 21

Figure 5: Overview of the closure phase (source: ECB) 23

9 Annexes

9.1 Annex I: list of acronyms

Table 1: LIST OF ACRONYMS

Acronym	Description
BIA	Business Impact Analysis
BT	Blue team
BTTR	Blue Team Test Report
CAP	The Code of Private Insurance (Decree Law 209/2005)
CERTFin	Italian Financial Computer Emergency Response Team
CIISI-EU	Pan-European Cyber Information and Intelligence Sharing Initiative
CT	Control Team
CTL	Control Team Lead
DORA	Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector, amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011
ECRB	Euro Cyber Resilience Board for pan-European Financial Infrastructures
CF/s	Critical or Important Function/s
GTL	Generic Threat Landscape
ID	Initiation Documents
NDA	Non-Disclosure Agreement
PT	Purple Teaming
RP	Remediation Plan
RTS on TLPT	Commission Delegated Regulation (EU) 2025/1190 of 13 February 2025 supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying the criteria used for identifying the financial entities required to perform threat-led penetration testing, the requirements and standards governing the use of internal testers, the requirements in relation to the scope, testing methodology and approach for each phase of the testing, results, closure and remediation stages and the type of supervisory and other relevant cooperation needed for the implementation of TLPT and for the facilitation of mutual recognition
RTT	Red Team Tester
RTTP	Red Team Test Plan
RTTR	Red Team Test Report
SSD	Scope Specification Document

Table 1: LIST OF ACRONYMS

Acronym	Description
SSM	Single Supervisory Mechanism
TCT	TIBER Cyber Team or TLPT Cyber Team
TI	Threat Intelligence
TIBER	Threat Intelligence-Based Ethical Red Teaming
TLPT SC	TLPT Steering Committee for the Italian financial sector
TIP	Threat Intelligence Provider
TKC	TIBER-EU Knowledge Centre
TLPT	Threat-Led Penetration Testing
TM	Test Manager
TSR	Test Summary Report
TTIR	Targeted Threat Intelligence Report
TTPs	Tactics, Techniques and Procedures
TUB	Consolidated Law on Banking (Decree Law 385/1993)
TUF	Consolidated Law on Finance (Decree Law 58/1998)

9.2 Annex II: additional documentation and main meetings

For the execution of a test, all the relevant stakeholders rely on a set of supporting documents that provide additional and more specific guidance or serve as templates to be used throughout the testing process.

Unless there are some national specificities, for which the TCT prepares and provides dedicated documents and templates, reference is made to the materials developed at the European level under the TIBER-EU framework, as listed in Table 2 below.

Table 3 lists the main meetings provided for by the methodology.

Further information may be requested at: tiber-it@bancaditalia.it.

Table 2: ADDITIONAL DOCUMENTATION AVAILABLE ON THE ECB'S WEBSITE

#	Title
1	TIBER-EU Framework: How to implement the European framework for Threat Intelligence-Based Ethical Red teaming
2	TIBER-EU Guidance for Service Provider Procurement
3	TIBER-EU Control Team Guidance
4	TIBER-EU Purple Teaming Guidance
5	TIBER-EU Initiation Documents Guidance
6	TIBER-EU Scope Specification Document Guidance
7	TIBER-EU Targeted Threat Intelligence Report Guidance
8	TIBER-EU Red Team Test Plan Guidance
9	TIBER-EU Red Team Test Report Guidance
10	TIBER-EU Blue Team Test Report Guidance
11	TIBER-EU Remediation Plan Guidance
12	TIBER-EU Test Summary Report Guidance
13	TIBER-EU Attestation Guidance

Table 3: MAIN MEETINGS

#	List of the main meetings	Parties involved
1	Notification	TM, representatives of the financial entity (e.g. CTL and/or future CT members)
2	Initiation	TM, CTL and future CT members
3	Scoping	CTL, CT, TM, TIP and/or RTT (if already appointed)
4	Launch	CTL, CT, TM, TIP and RTT
5	Selection Scenario	CTL, CT, TM, TIP and RTT
6	Targeted threat intelligence	CTL, CT, TM, TIP and RTT
7	Red Team Test Plan	CTL, CT, TM, RTT and TIP (if necessary)
8	Weekly meetings or test updates	CTL, CT, TM, RTT and TIP (if necessary)
9	Replay Exercise	CTL, CT, BT, RTT and TM (if necessary)
10	PT Exercise	CTL, CT, BT, RTT
11	360-degree Feedback meeting	TM, CTL, CT, BT, TIP, RTT and TCT (if necessary)