EUROPEAN CENTRAL BANK

EUROSYSTEM

TIBER-EU FRAMEWORK

How to implement the European framework for Threat Intelligence-based Ethical Red Teaming

May 2018

Contents

1 Executive summary

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

1.1 What is TIBER-EU?

TIBER-EU is a common framework that delivers a controlled, bespoke, intelligence-led red team test of entities’ critical live production systems. Intelligence-led red team tests mimic the tactics, techniques and procedures (TTPs) of real-life threat actors who, on the basis of threat intelligence, are perceived as posing a genuine threat to entities. An intelligence-led red team test involves the use of a variety of techniques to simulate an attack on an entity’s critical functions (CFs) and underlying systems (i.e. its people, processes and technologies). It helps an entity to assess its protection, detection and response capabilities.

1.2 What are the core objectives of TIBER-EU?

As the appetite grows for authorities in different jurisdictions to develop national intelligence-led red teaming frameworks, there is a risk that incompatible frameworks could emerge which could lead to an unnecessary duplication of effort. Multiple frameworks potentially represent a substantial burden for entities (financially and otherwise). They also give rise to the risk of unnecessarily exposing sensitive information and in addition may lead to inconsistent results. TIBER-EU therefore has the following core objectives:

- enhance the cyber resilience of entities, and of the financial sector more generally;
- standardise and harmonise the way entities perform intelligence-led red team tests across the EU, while also allowing each jurisdiction a degree of flexibility to adapt the framework according to its specificities;
- provide guidance to authorities on how they might establish, implement and manage this form of testing at a national or European level;
- support cross-border, cross-jurisdictional intelligence-led red team testing for multinational entities;
- enable supervisory and/or oversight equivalence discussions where authorities seek to rely on each other’s assessments carried out using TIBER-EU, thereby reducing the regulatory burden on entities and fostering mutual recognition of tests across the EU;

- create the protocol for cross-authority/cross-border collaboration, result sharing and analysis.

1.3 What is the purpose of this framework document and who is it for?

This framework document provides an overview of TIBER-EU and how it will be implemented across the EU, with details of the key phases, activities, deliverables and interactions involved in a TIBER-EU test. The document is aimed at: authorities responsible for the adoption, implementation and management of the TIBER-EU framework at national and European levels; entities looking to undertake TIBER-EU tests; supervisors and overseers of those entities; organisations interested in providing cyber threat intelligence services under TIBER-EU; and organisations interested in providing red team testing services under TIBER-EU.

The TIBER-EU framework has been designed for use at entities which are part of the core financial infrastructure, whether at national or at European level. However, it can also be used for any type or size of entity across the financial and other sectors. It is up to the relevant authorities – in consultation with the entities under their responsibility – to determine whether and when TIBER-EU tests are to be performed.

1.4 Who are the key stakeholders involved in the adoption and implementation of TIBER-EU tests?

The implementation of TIBER-EU, whether at national or European level, is a multi-stakeholder process. The TIBER-EU framework is designed to be adopted by relevant authorities in any jurisdiction, on a voluntary basis and from a variety of perspectives, namely as a supervisory or oversight tool, for financial stability purposes, or as a catalyst. The relevant authorities will then consider which entities could be invited to participate in the test.

The unique aspect of TIBER-EU is the objective of facilitating testing for entities which are active in more than one jurisdiction and fall within the regulatory remit of several authorities. In these circumstances, the TIBER-EU framework permits two testing approaches: collaborative cross-authority testing under the direction of the lead authority; and/or a test managed by one of the relevant authorities (ideally, the lead authority of the entity), which can be mutually recognised and provide assurance to relevant authorities in other jurisdictions, provided the core requirements of the TIBER-EU framework have been met.

Although several entities already conduct red team testing with dedicated internal red teams, authorities will only recognise a TIBER-EU test if it is conducted by independent third-party providers (i.e. external threat intelligence (TI) and red team (RT) providers). An external tester provides a fresh and independent perspective, which may not always be feasible with internal teams that have grown accustomed

to the internal systems, people and processes. Furthermore, external providers may have more resources and up-to-date skills to deploy, which would represent additional benefits for the entity.

The TIBER-EU test requires the involvement of the following parties: the entity, which is responsible for managing the end-to-end test and ensuring that all risk management controls are in place to facilitate a controlled test; the authorities, who oversee the test and ensure they are conducted in the right spirit and in accordance with the requirements of the TIBER-EU framework; and external TI and RT providers, who conduct the test. Overall, it is the respective entity – and not the authorities – that bears the first and final responsibility for conducting the test.

For the TIBER-EU test to provide meaningful results, it is important that all stakeholders work closely together, in a spirit of trust and cooperation, as the test will not result in a pass or fail, but will provide all parties with an insight into strengths and weaknesses, and enable the entity to learn and evolve to a higher level of cyber maturity.

1.5 What is the TIBER-EU test process?

The TIBER-EU framework sets out a mandatory three-phase process for an end-to-end test. The preparation phase (which includes engagement & scoping and procurement) represents the formal launch of the test. The teams responsible for managing the test are established, the scope of the test is determined and attested by the entity's board and validated by the authority (e.g. overseers/supervisors), and the TI and RT providers are procured by the entity to carry out the test.

In the testing phase (which includes threat intelligence and red teaming), the TI provider prepares a Targeted Threat Intelligence Report (TTI Report) on the entity, setting out attack scenarios for the test and useful information on the entity. The report will be used by the RT provider to carry out an intelligence-led red team test of specified critical live production systems, people and processes that underpin the entity's CFs.

Finally, the closure phase (which includes remediation planning and result sharing) requires the RT provider to draft a Red Team Test Report, which will include details of the approach taken to the testing, along with the findings and observations from the test. Where necessary, the report will include advice on areas for improvement in terms of technical controls, policies and procedures, and education and awareness. The main stakeholders will now be aware of the test, and should replay the executed scenarios and discuss the issues uncovered during the test. The entity will take on board the findings, and agree and finalise a Remediation Plan, in close consultation with the supervisor and/or overseer; the process of the test will be reviewed and

discussed, and the key findings from the test will be shared with other relevant stakeholders.[1]

1.6 What are the risks of the TIBER-EU test?

There are inherent elements of risk associated with a TIBER-EU test for all parties due to the criticality of the live production systems, people and processes involved in the tests. The possibility of causing a denial-of-service incident, an unexpected system crash, damage to critical live production systems, or the loss, modification, or disclosure of data, highlights the need for active and robust risk management. In line with the potential risk of the test, the TIBER-EU framework places high priority on establishing robust risk management controls throughout the entire process of the test to ensure it is conducted in a controlled manner.

To ensure a controlled and safe test, the roles and responsibilities of all stakeholders must be clearly established and understood. However, it is equally critical that the test is conducted without the prior knowledge of the entity (except for a small number of staff members) in order to gain a true picture of the entity's protection, detection and response capabilities.

In addition, to ensure that the test is conducted to the highest standards, the external TI and RT providers must meet specified requirements and ideally be accredited and certified by appropriate bodies. The requirements under the TIBER-EU framework have been made deliberately stringent to ensure that only the best and most qualified personnel conduct such sensitive tests on CFs.

1.7 What are the next steps?

As jurisdictions consider adopting the TIBER-EU framework, the relevant authorities within the jurisdictions are encouraged to engage with each other to determine how best to adopt and implement it.[2] Entities are encouraged to liaise with their relevant authorities and work closely with them to establish a framework that will enhance the cyber resilience of their sector. Meanwhile, TI and RT providers are encouraged to consider their resources and capabilities to ensure that they meet the required standards in delivering bespoke, intelligence-led red team tests for entities.

The TIBER-EU framework envisages a collaborative approach, with all stakeholders working closely together and learning from each other. To this end, the implementation of the TIBER-EU framework will be monitored by the TIBER-EU Knowledge Centre (TKC). In addition, the framework will evolve to reflect learnings from all jurisdictions and allow improvements to be integrated where necessary.

---

1 Detailed technical findings regarding weaknesses will only be made available to the respective entity; a Test Summary Report on the findings (including a Remediation Plan) will be made available to the relevant authorities (supervisor and/or overseer).

2 This will result in specific TIBER-XX Implementation Guides, in which XX stands for the respective country code (e.g. DE, DK, BE, etc.).

Any further enquiries about TIBER-EU should be directed to TIBER-EU@ecb.europa.eu.

2 Introduction

2.1 Background

The financial system is a complex network of participants from different environments and shared technologies, with a large volume of information flowing through the network. It includes all types of entities, information, technologies, rules and standards that enable financial intermediation. Efficient, safe and reliable infrastructure enables entities and others to expand their offering of financial services to the broader economy. Within this context, there are highly sophisticated cyber threat actors who target the most vulnerable links in this network, and so it is critical that entities reduce their vulnerabilities at every point and strengthen their overall resilience. This requires diverse, layered approaches, solutions and tools. Intelligence-led red team testing is one such tool to help entities test and enhance their protection, detection and response capabilities.

TIBER-EU enables authorities to work with entities under their responsibility to put in place a programme for testing and improving their resilience against sophisticated cyber attacks.

For the purposes of the TIBER-EU framework, “entities” means:

“payment systems, central securities depositories, central counterparty clearing houses, trade repositories, credit rating agencies, stock exchanges, securities settlement platforms, banks, payment institutions, insurance companies, asset management companies and any other service providers deemed critical for the functioning of the financial sector”.

2.2 Purpose of this framework document

This framework document provides an overview of how TIBER-EU will be implemented across the EU. It explains the key phases, activities, deliverables and interactions involved in a TIBER-EU test. This document is not a detailed prescriptive method, but an overarching framework which should be complemented with other relevant TIBER-EU materials (as set out in Annex III).

2.3 Who is this framework document for?

This framework document is aimed at:

- authorities responsible for the adoption, implementation and management of the TIBER-EU framework at national and European levels;
- entities looking to undertake TIBER-EU tests;

- supervisors and overseers of those entities;
- organisations interested in providing cyber threat intelligence services under TIBER-EU;
- organisations interested in providing red team testing services under TIBER-EU.

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

2.4 What is TIBER-EU?

TIBER-EU is a common framework that delivers a controlled, bespoke, intelligence-led red team test of entities' critical live production systems.

The aims of TIBER-EU are as follows: to improve the protection, detection and response capabilities of entities; to enhance the resilience of the financial sector; and to provide assurance to the authorities about the cyber resilience capabilities of the entities under their responsibility.

A common framework…

As the appetite grows for different jurisdictions to develop national intelligence-led red teaming frameworks, there is a risk that incompatible frameworks could emerge which could lead to an unnecessary duplication of effort. Multiple frameworks potentially represent a substantial burden for entities (financial and otherwise). They also give rise to the risk of unnecessarily exposing sensitive information, and may additionally lead to inconsistent results.

TIBER-EU therefore has the following core objectives:

- enhance the cyber resilience of the entities, and the financial sector more generally;
- standardise and harmonise the way entities perform intelligence-led red team tests across the EU, while also allowing each jurisdiction a degree of flexibility to adapt the framework according to its specificities;
- provide guidance to authorities on how they might establish, implement and manage this form of testing at a national and European level;
- support cross-border, cross-jurisdictional intelligence-led red team testing for multinational entities;
- enable supervisory and/or oversight equivalence discussions where authorities seek to rely on each other's assessments carried out using TIBER-EU, thereby

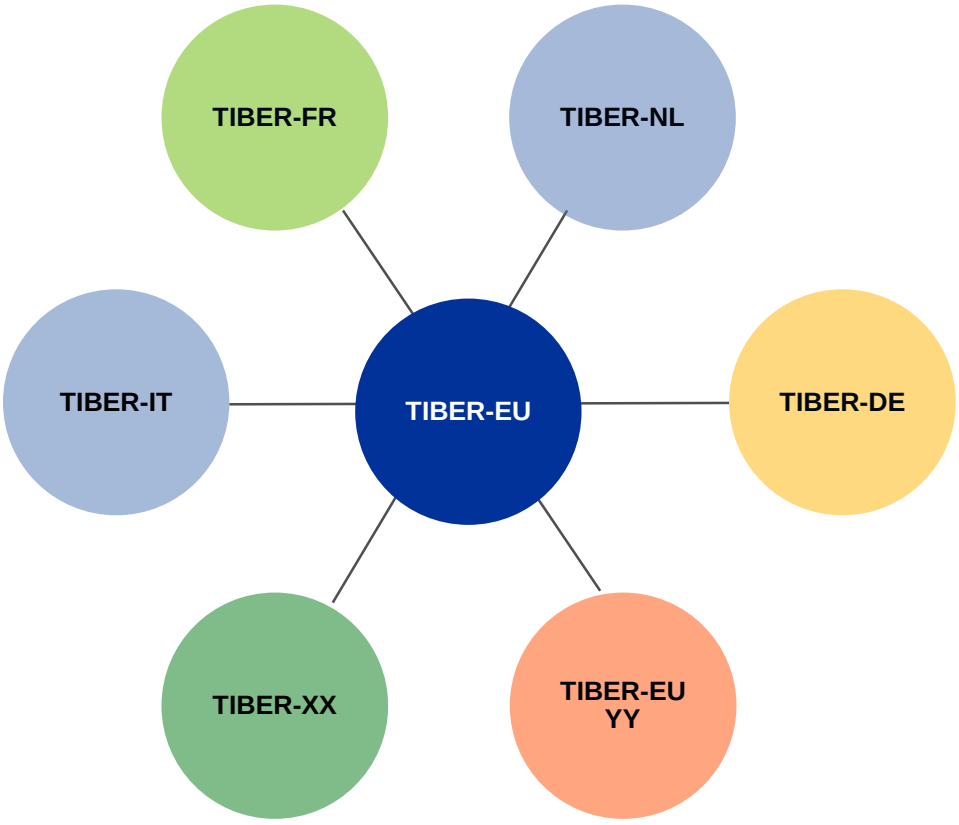
reducing the regulatory burden on entities and fostering mutual recognition of tests across the EU;

- create the protocol for cross-authority/border collaboration, result sharing and analysis.

… with national implementation…

The TIBER-EU framework acts as a central hub. Each jurisdiction can adopt the framework at a national or European level, applying it in a manner which suits its specificities. If the framework is adopted at a national or European level, there should be an accompanying national (TIBER-XX) or European (TIBER-EU YY) Implementation Guide, with XX representing the two-letter ISO 3166-1 country code and YY the European authority. This is shown in the following diagram:

Figure 1
TIBER-EU framework and national/European implementation guides



The framework offers a level of flexibility which allows for national implementations to accommodate a wide range of institutional set-ups, legal mandates and market structures. Some authorities may implement this framework from an oversight and/or supervisory perspective, while others may choose to implement the framework from a financial stability perspective.

… developed with input from the industry

To develop TIBER-EU, authorities have:

- consulted with entities to elicit support and to take advice;
- engaged with the red team providers (RT providers) in the EU to develop a scheme that is sympathetic to the concerns raised by the financial services industry and the risks associated with testing critical technology assets;
- engaged with the threat intelligence providers (TI providers) in the EU to seek their advice and establish good practices, which will facilitate the provision of intelligence required to identify current threat actors engaged in attacks against critical EU entities;
- worked closely with jurisdictions[3] [4] which have already developed, or are developing, similar intelligence-led ethical red teaming frameworks.

This collaboration has formed the basis for defining the TIBER-EU framework, which, with the support of the financial industry, puts in place measures to provide confidence that targeted tests can be conducted on critical technology assets while minimising risk. The TIBER-EU framework harnesses the threat intelligence and threat scenarios from the TI providers to develop a Red Team Test Plan which is executed by red team testing companies.

2.5 Why intelligence-led red team testing?

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

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

Intelligence-led red team tests mimic the tactics, techniques and procedures (TTPs) of advanced threat actors who are perceived by threat intelligence as posing a genuine threat to entities.

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

---

[3] See Financial sector continuity. In respect of CBEST see also creative commons.

[4] See DNB publishes TIBER ethical hacking guide for financial core payment institutions.

The idea of TIBER-EU is to:

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

TIBER-EU tests are to be performed without the knowledge of the target entity's security or response capability (i.e. Blue Team, BT). Only a small group from the entity, referred to as the White Team (WT), knows about the test. This is to ensure that the test can assess how effectively the target entity is able to protect its critical systems, and how effectively it can detect and respond to attacks.

Given the nature of a TIBER-EU test and the critical nature of the live production systems and other connected environments being tested, the framework sets out a number of risk management activities to ensure a controlled test.

2.6 Additional information

Any further enquiries about TIBER-EU should be directed to TIBER-EU@ecb.europa.eu.

3 Adoption and implementation of TIBER-EU

3.1 Implementation of the TIBER-EU framework

For the implementation of the TIBER-EU framework, certain overarching governance structures and processes must be put in place, adopted at either national or European level and followed to ensure that the framework can be implemented effectively across the EU.

3.2 Authorities involved

The adoption of the TIBER-EU framework by authorities and jurisdictions is voluntary. At the inception, authorities wishing to implement a TIBER-EU framework in their jurisdictions are encouraged to liaise with all relevant authorities in the financial sector. These may include:

- central banks;
- supervisory authorities;
- intelligence agencies;
- relevant ministries.

The TIBER-EU framework may be adopted at a national level, or by EU institutions and authorities. However, national or European implementation of TIBER-EU need not be limited to the financial sector alone. Should a jurisdiction wish to involve other sectors (such as telecommunications or utility companies), the TIBER-EU framework does not prevent it from doing so. As such, the framework is entity-agnostic and sector-agnostic.

The various authorities should discuss the potential adoption of the framework, how it should be set up, the entities that it will apply to, the timelines, and the general organisation and resources required to implement the framework.

3.3 Mandate and adoption

If a jurisdiction decides to adopt the TIBER-EU framework, its national implementation must be formally adopted by the Board of an authority, ideally the central bank of the European System of Central Banks (ESCB). The TIBER-EU Knowledge Centre (described in more detail in Section 3.8) must be officially informed that a national or European implementation of TIBER-EU has been launched.

Adoption of the TIBER-EU framework can be driven in collaboration with market participants to serve as a catalyst. The framework may also be adopted for the purposes of financial stability. Alternatively, it may be adopted as an oversight and/or supervisory requirement.

In these cases, the implementation of the TIBER-EU framework must be in accordance with the mandatory requirements, as set out in Annex I.

3.4 Establishment of TIBER-EU

Preferably, one of the relevant authorities should take ownership of the national or European TIBER-EU implementation. This authority develops the national (TIBER-XX) or European (TIBER-EU YY) Implementation Guide, organises the programme, liaises with the other authorities and coordinates the joint work. One of the relevant authority's board members should take ownership of this programme of activities.

For each implementation, the relevant authorities should work together to reach agreement on the form that the national framework will take and how it will be implemented in their jurisdictions. Each implementation of TIBER-EU must ensure that all the core foundational concepts and approaches are adopted and implemented; however, each jurisdiction is free to adopt and implement further optional elements at its own discretion.

The authority that owns the TIBER-XX framework within its jurisdiction must publish on its website the official TIBER-XX Implementation Guide applicable to its jurisdiction and take measures to explain the adoption of the framework to the relevant market participants.

3.5 Legal and compliance

During the process of establishing the national or European implementation of TIBER-EU, authorities should conduct a review of existing laws and regulations at a national and European level to ensure that the framework, methodologies and processes do not contravene any law and the implementation of the framework remains legally compliant.

Furthermore, it is the responsibility of the entities, TI providers and RT providers to ensure that they conduct tests within the remit of all laws and regulations, and appropriate risk management controls (e.g. contracts) are in place to enforce this.

During the TIBER-EU process, there are a number of activities that may be performed to fully replicate a real-life attack. Such activities require due consideration and evaluation in the context of existing laws and regulations, and may include the following:

- gathering open-source intelligence (OSINT) data on the target entity (publicly available information);

- gathering OSINT data on the entity's suppliers (publicly available information);
- gathering data from other intelligence sources (e.g. government sharing platforms, etc.) relating to the target entity;
- gathering any data on the entity, its suppliers, its employees and/or its customers found on the dark web;
- deployment of people into the entity under various guises to gather intelligence;
- using targeting data gathered in the threat intelligence phase to create email, telephone and in-person ruses as part of a scenario;
- gathering data on employees and customers of the entity;
- gathering account and password data from employees and service providers of the target entity.

The above are suggested activities to consider, but the list is not exhaustive. Authorities should ensure that a thorough legal analysis is carried out, using appropriate legal expertise, to determine the legal constraints when performing the test. These should be clearly set out in the documentation at national and European level.

Simultaneously, all entities, TI providers and RT providers should consider and act in accordance with the legal constraints of each jurisdiction.

The above activities will be performed under a contractual agreement with the full consent of the respective entity. This will mitigate beforehand many of the legal concerns which may potentially arise.

3.6 Governance by authorities

For each national and European implementation of the TIBER-EU framework, the relevant authorities should establish the appropriate governance structures and allocate resources to:

- ensure that the framework is formally owned by senior personnel;
- manage, operationalise and monitor its implementation by staff with the requisite skills;
- continuously update the framework in the light of lessons learned from its implementation, and in collaboration with other authorities via the TIBER-EU Knowledge Centre.

3.7 The TIBER Cyber Team

The authorities who decide to be involved in an implementation of TIBER-EU should set up a centralised TIBER Cyber Team (TCT) that brings together their TIBER knowledge and capabilities at national or European level. The TCT facilitates the different TIBER-XX/TIBER-EU YY tests across the sector, provides support and specialist knowledge to White Team Leads (WTLs, responsible for the entity's test management), acts as the contact point for all external enquiries and supports the overseers and supervisors during and/or after the tests (if the overseers and supervisors are not included in the TCT).

The TCT is also responsible for maintaining the national and European TIBER Implementation Guide and for developing it further according to national or European needs. In addition, national and European TCTs may liaise with other TCTs in other TIBER jurisdictions.

There are various ways in which the TCT could be set up, ranging from one authority alone (acting as a central point from which experts are sent to support overseers and supervisors) to a centralised team consisting of experts from all relevant authorities (including overseers and supervisors), with a clear anchor at one of the authorities. Most importantly, the TCT is one of the crucial operational controls in performing a test on critical live production systems and helps ensure a uniform, high-quality test containing all the mandatory elements.

When setting up the TCT, each jurisdiction should carefully consider the resources required, based on the number of entities that will be subject to testing, and ensure that staff on the TCT are appropriately skilled in project management and have the requisite knowledge on cyber security and the entities being tested.

During a TIBER-EU test, the TCT holds the right to invalidate a test for TIBER recognition if it suspects that the entity is not conducting the test in the right spirit and in accordance with the requirements of the TIBER-EU framework.

3.8 TIBER-EU Knowledge Centre

A centralised TIBER-EU Knowledge Centre (TKC), hosted by the ECB[5], will be set up to enhance further collaboration among the national and European TCTs so that they can benefit from multiple potential implementations of the TIBER-EU framework. The core objectives of the TKC will be to:

- facilitate knowledge exchange and foster collaboration among national and European TCTs;
- support national and European implementations and provide a central depository of materials for jurisdictions;

[5] In close cooperation with the national central banks of the European System of Central Banks (ESCB).

- provide authorities with training on the development, implementation and management of the TIBER-EU framework;
- monitor the national and European implementations (thereby ensuring legitimacy of mutual recognition), collect feedback, reflect on lessons learned, disseminate information to national jurisdictions as appropriate, and maintain and continually develop the TIBER-EU framework;
- promote information sharing, mutual collaboration and other actions to enhance overall cyber resilience within the EU;
- liaise with other authorities using intelligence-led red team testing in order to promote international uniformity and quality;
- provide feedback to the sector within the relevant fora (e.g. Euro Cyber Resilience Board for pan-European Financial Infrastructures), where necessary and appropriate.

3.9 Identification of entities and relevant authorities

Participation of the entities in the TIBER-EU scheme may be either voluntary or mandatory; this is left to the discretion of the relevant national or European authorities. As a rule, the lead authority should initiate and oversee the conduct of TIBER-EU tests on entities under its responsibility.

For the purposes of the TIBER-EU framework, a lead authority means: “the authority with the primary responsibility for overseeing and supervising a relevant entity”.

Following the adoption of the TIBER-EU framework at a national or European level, each lead authority should decide which entities should be invited to undertake, or must undertake, a TIBER-EU test, and by when. Entities differ in size, complexity and reach. Therefore, authorities should look to include entities which are important to the financial stability of the jurisdiction because of the critical functions (CFs) they perform. That said, the TIBER-EU framework can be applied to all types and sizes of entities.

3.10 Cross-jurisdictional activities

Within the EU, several entities may operate their business across borders, with a presence in multiple jurisdictions. In such circumstances, each lead authority will need to determine and agree which other “relevant authorities” are potential key stakeholders for the given entity.

In cases where an entity is active in more than one jurisdiction, the TIBER-EU framework permits the relevant authorities to take one or both of the following approaches to cross-jurisdictional activities.

- Relevant authorities should, ideally, work together in a collaborative manner under the direction of the lead authority.
- A test managed by one of the relevant authorities (ideally, the lead authority of the entity) should be conducted in accordance with the core requirements of the TIBER-EU framework in order to be mutually recognised and to provide assurance to the relevant authorities in other jurisdictions. In such cases, there must be mutual agreement, right from the outset, on the identity of the other relevant authorities.

The lead authority should consider a number of elements when determining the identity of the other relevant authorities. Elements to be considered include:

- the geographical location of the entity;
- the organisational and legal structure of the entity (e.g. group structure);
- the geographical location of the underlying critical service provider (which may be within the scope of the testing activities) and its lead authority;
- the oversight and/or supervisory arrangements for the entity (e.g. cooperative oversight arrangements, joint supervisory teams, etc.).

In some circumstances, there may be an authority that is implementing the framework at national level (TIBER-XX) and is seeking to conduct a test on a cross-border entity whose lead authority has not yet implemented the TIBER-EU framework at national level, or intends to implement it in the future. In such circumstances, the relevant authority should contact the lead authority and discuss how the test should be conducted under its TIBER-XX implementation. Collaboration in these situations is beneficial, as it allows the entity in question to conduct the test within a recognised framework, involving all relevant authorities, and with full scope. In addition, such collaboration avoids delays in the testing process.

The process for identifying and engaging with other relevant authorities can also be an iterative process. For example, during the scoping process the different stakeholders may deduce that a CF is located in another jurisdiction. In these circumstances, it may then be necessary to contact and liaise with other relevant authorities before commencing any activity.

Overall, the key to facilitating cross-border testing is mutual trust between lead authorities, other relevant authorities and the entities. In all cases, the stakeholders should use sound judgement, foster a spirit of collaboration, and show a willingness to find a workable process that allows effective testing to be conducted with the right scope.

To illustrate the principles described above, an example is given in Figure 2 below. The entity X has its head office in Germany and is subject to oversight/supervision by a German authority as the lead authority. However, the entity is also present in the Netherlands and Belgium and is systemically important to all three jurisdictions.

Figure 2

Example of an entity's European presence

In this case, the German authority may deem entity X to be important and seek to include it within the scope of its testing regime. The German authority should consider which other relevant authorities may have an interest in the testing of the entity, and reach out to the relevant TCT. Equally, the other relevant authorities (in this case Belgium and Netherlands), may consider entity X to be important for its jurisdictions, and approach the German authority to initiate a test.

The TCT responsible for TIBER-DE would liaise in this case with the TCTs responsible for TIBER-NL and TIBER-BE. In such a scenario, the three authorities might consider collaborating on a joint test on entity X, where members of the German, Dutch and Belgian TCTs work together throughout the test; or the authorities in the Netherlands and Belgium might decide to rely solely on the German-led test and seek assurance from this process, as long as the core elements of the TIBER-EU framework were followed.

3.11 Mutual recognition

In the highly interconnected European financial system, it is likely that numerous authorities will require assurance on the cyber resilience of a single entity. TIBER-EU provides an efficient solution to this problem by ensuring mutual recognition of TIBER tests, provided that these comply with all mandatory requirements of the TIBER-EU framework.

A precondition for mutual recognition is that each test must comply with all the mandatory requirements of the TIBER-EU framework, which are set out in Annex I. At the end of each test, the board of the entity, the TI provider and the RT provider should sign an attestation confirming that the test was conducted in accordance with the mandatory requirements of the TIBER-EU framework. This will provide the legitimacy for mutual recognition. Furthermore, the lead authority should confirm to other relevant authorities that it oversaw the test conducted. If the lead authority considers that the conduct of the test was not in line with the requirements and spirit of the TIBER-EU framework and the national or European Implementation Guide, it has the right to invalidate the test for TIBER-EU recognition and mutual recognition.

As noted above, for some entities, the test might be managed by a small number of authorities together. However, in some cases, the entity might be a more complex group structure with multiple subsidiaries or branches, and so there might be a significant number of relevant authorities. In these circumstances, managing a large-scale test, with so many relevant stakeholders, might be inefficient and counter-productive. Consequently, the onus should be on the lead authority, entity and other relevant authorities (who seek assurance through a mutually recognised test) to negotiate the safe sharing of the results ex post.

3.12 External testing

Although several entities already conduct red team testing with dedicated internal red teams, authorities will only recognise a TIBER-EU test if it is conducted by independent third-party providers (i.e. external TI and RT providers).

Although the practice of internal red teams is encouraged, and entities should look to develop this capability, there are clear advantages to procuring an external party to conduct a TIBER-EU test. Most notably, an external tester provides a fresh and independent perspective, which may not always be feasible with internal teams that have grown accustomed to the internal systems, people and processes. Furthermore, external providers might have more resources and up-to-date skills to deploy, which would add value to the entity.

With this in mind, given the resources required and costs incurred, entities are not expected to conduct a TIBER-EU test too frequently.

4 High-level overview of the TIBER-EU process

4.1 Intelligence-led red teaming

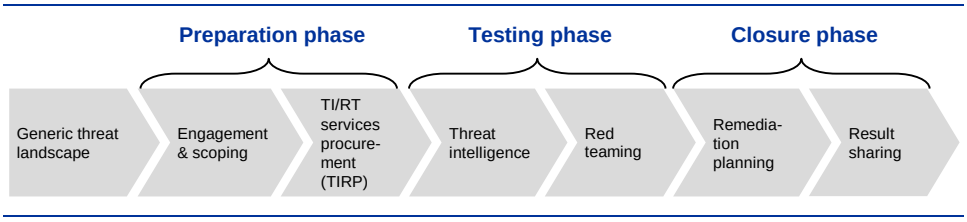
There are a range of different types of tests in the market today which help entities to improve their basic “cyber hygiene”. Among them, intelligence-led red teaming is one of the most comprehensive and insightful ways of testing the capabilities of an entity.

An intelligence-led red team test mimics the TTPs of real attackers on the basis of bespoke threat intelligence. In doing so, it looks to target the people, processes and technologies underpinning the CFs of an entity in order to test its protection, detection and response capabilities without their prior knowledge.

It allows the entity to understand its real-world resilience by stressing all elements of its business against the TTPs of the threat actors that are specific to their organisation. The intelligence-led red team test provides a comprehensive end-to-end understanding of weaknesses present in people, business processing, technology, and their associated intersection points, and provides a detailed threat assessment which can be used to further enhance the entity’s situational awareness.

All relevant stakeholders should adhere to the following process for each test, to ensure standardisation and harmonisation across all jurisdictions and implementations:

Figure 3
TIBER-EU process



4.2 Process overview

The TIBER-EU test process consists of three mandatory phases and one optional phase. Please note that some phases can and should overlap, as this helps to ensure the best possible test. The four phases are:

1. The generic threat landscape (GTL) phase – The GTL phase involves a generic assessment of the national financial sector threat landscape, outlining the specific roles of the entities (e.g. investment banks, commercial banks, payment systems, central counterparties, exchanges, etc.), identifying the relevant high-

end threat actors for the sector and the TTPs targeting these entities. The GTL will link these threat actors and the TTPs to the specific entities within the sector, and can be used as a basis for later attack scenario development. The GTL may be validated and reviewed by the relevant national intelligence agency if possible, and updated on an ongoing basis as new threat actors and TTPs emerge and pose a risk to the entity. The GTL phase is optional.

2. The preparation phase (which includes engagement & scoping and procurement) – During this phase, the following takes place: the engagement for the TIBER-EU test is formally launched; the teams responsible for managing the test are established; the scope of the test is determined, approved and attested to by the entity's board, and validated by the relevant authorities; and the TI and RT providers are procured to carry out the test. The preparation phase is mandatory for each implementation of the TIBER-EU framework.

3. The testing phase (which includes threat intelligence and red teaming) – During this phase, the procured TI provider prepares a Targeted Threat Intelligence Report (TTI Report) on the entity, setting out threat scenarios for the test and useful information on the entity. Here the TI provider works closely with the RT provider, and the targeted threat intelligence and reconnaissance phases overlap, with the GTL being used as the basis, if available. The TTI Report will be used by the RT provider to develop attack scenarios and execute an intelligence-led red team test of specified critical live production systems, people and processes that underpin the entity's CFs. The testing phase is a mandatory phase for each implementation of the TIBER-EU framework.

4. The closure phase (which includes remediation planning and result sharing) – During this phase, the RT provider drafts a Red Team Test Report, which will include details of the approach taken to the testing and the findings and observations from the test. Where necessary, the report will include advice on areas for improvement in terms of technical controls, policies and procedures, and education and awareness. The main stakeholders will now be aware of the test, and should replay the executed scenarios and discuss the issues uncovered during the test. The entity will take on board the findings, and will agree and finalise a Remediation Plan in close consultation with the supervisor and/or overseer; the process of the test will be reviewed and discussed; and the key findings from the test will be shared with other relevant authorities. Approval to close the test should be obtained from the relevant authorities once a Remediation Plan has been agreed. The closure phase is mandatory for each implementation of the TIBER-EU framework.

5 Roles and responsibilities in the TIBER-EU test

5.1 Roles and responsibilities

A TIBER-EU test requires the involvement of a number of different stakeholders with clearly defined roles and responsibilities. All main stakeholders involved in a TIBER-EU test should be well informed about their respective roles and responsibilities to ensure that:

- the test is conducted in a controlled manner;
- there is a clear protocol for the flow of information across all relevant stakeholders throughout the test;
- the information flow protocol is clear on how information will be stored and shared between stakeholders.

For more clarity on the roles and responsibilities of the different stakeholders involved in the overall process of a TIBER-EU test, a Responsibility Assignment (RACI) Matrix is included in Annex II.

5.2 Main stakeholders

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

- the TCT and Team Test Manager (TTM);
- the WT and WTL;
- the BT;
- the TI provider;
- the RT provider;
- the relevant governmental intelligence agency or national cyber security centre.

5.3 Test management

The end-to-end conduct of a TIBER-EU test is the responsibility of the entity. The two key stakeholders involved in project managing the test are the TCT as the authority and the WT as the entity. Both the TCT and WT should have extensive knowledge of the entity's business model, functions and services.

The WT and WTL:

For each TIBER-EU test, there should be a WT, with a dedicated WTL from the entity. The WTL coordinates all test activity including engagement with the TI/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.

The TCT and TTM:

For each TIBER-EU test, there should be a TTM from the TCT who has experience in the relevant sector, as well as cyber expertise and project management experience. The role of the TTM is to make sure that the entity undertakes the test in a uniform and controlled manner, and in accordance with the TIBER-EU framework. Given the importance of the TTM's role, a backup TTM is strongly advised.

Responsibilities of the WTL and TTM:

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

Responsibility for the overall planning and management of the test lies with the entity. The WTL is responsible for determining and finalising the scope, scenarios and risk management controls for the test, ensuring that they have been approved and attested by the board and validated by the TTM. In addition, the WTL should coordinate all test activity including engagement with the TI/RT providers. The WTL should ensure that the TI/RT providers' project plans are factored into the entity's overall project planning for the TIBER-EU test.

If there are significant deviations in the original planning, this should be discussed with the TTM. It is critical that all relevant stakeholders keep each other informed at all stages to ensure that the test runs smoothly and that any issues, resourcing constraints, etc. can be addressed in a timely fashion.

The TTM should agree on the scope and the scenarios, and ensure that the test is executed according to plan and that it conforms to TIBER-EU test standards and all relevant requirements (as set out in Annex I), which is important for possible recognition by other jurisdictions.

Although the WTL is the primary contact for the TI and RT providers, the TTM should also have direct access to the providers when required. Where there are crucial decisions to be made (e.g. deviations during the test from the agreed scope), or where differences of opinion arise, both the WTL and TTM should have a formal escalation line to their respective superiors. 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;
- the head of the TCT, the board member at the lead authority for TIBER-XX, or any other appropriate senior personnel with sufficient decision-making authority.

The TTM is independent from the WT and is not accountable for the WT's actions, the running of the test, the outcomes or the remediation planning. It is the responsibility of the WT to ensure that a fit and proper test is conducted in line with the requirements of the TIBER-XX framework and that risks are managed throughout all phases.

The BT:

For each TIBER-EU test, the BT comprises all staff at the entity who are not part of the WT. It is critical that the BT be completely excluded from the preparation and conduct of the TIBER-EU test. During the closure phase, when the BT is informed about the conduct of the test, only the relevant and most appropriate members of the BT should participate in the replay and follow-up.

5.4 Test implementation

For the end-to-end TIBER-EU test, there are two key stakeholders that have a role in its implementation. These are the TI and RT providers.

The TI provider:

The TI provider should provide threat intelligence to the entity in the form of a TTI Report. TI providers should use multiple sources of intelligence to provide an assessment that is as accurate and up to date as possible. The TTI Report sets out the threat scenarios that can be used by the RT provider to develop attack scenarios for the red team test.

The TI provider must demonstrate willingness and the ability to share its deliverables (once approved by the entity) with its red team testing counterpart for review and comment and demonstrate a willingness to work with the RT provider during the remainder of the TIBER-EU test. This includes 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 into the final report issued to the entity.

The RT provider:

The RT provider plans and executes a TIBER-EU test of the target systems and services, which are agreed in the scope. This is followed by a review of the test and issues arising, culminating in a Red Team Test Report drafted by the RT provider.

The RT provider should expand on and execute the established threat scenarios identified by the TI provider and approved by the entity. The threat scenarios are developed from an attacker's point of view. The RT provider should indicate various creative options in each of the attack phases based on the various TTPs used by advanced attackers. This is in order to anticipate changing circumstances or in case other attack methods do not succeed during the test. The scenario development is a creative process, and TTPs should not simply mimic scenarios seen in the past but should look to combine the TTPs of various relevant threat actors. The RT provider should aim to assess the cyber resilience posture of the entity in the light of the threat it faces.

The RT provider should follow a rigorous and ethical red team testing methodology, and should meet the minimum requirements defined under the TIBER-EU framework. The rules of engagement and specific testing requirements should be established by the RT provider and the entity.

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

The relevant governmental intelligence agency or national cyber security centre:

In many jurisdictions, there may be a governmental intelligence agency or national cyber security centre, or equivalent. In such jurisdictions, the authorities may decide to engage with these bodies and include them in the TIBER-XX process. The intelligence agency or cyber security centre may provide insight on the threat intelligence process, and look to enrich the individual TTI Reports using their internal knowledge. It is left to the discretion of the national authorities to determine the role of the intelligence agency or cyber security centre, and to take the relevant steps to interact and engage with them.

6 Risk management for TIBER-EU tests

6.1 Risk management

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

The entity is responsible for implementing appropriate controls, processes and procedures to ensure that the test is carried out with sufficient assurances for all stakeholders that risks will be identified, analysed and mitigated according to best practices in risk management.

6.2 Risk assessment

The entity should conduct a risk assessment prior to the test. Throughout the conduct of the TIBER-EU test, the entity should ensure that it gives due consideration to the risks associated with the test. It should take the right risk management precautions throughout, in line with its existing risk management framework. To reduce the risks associated with testing, sufficient planning and coordination must take place before and during the test.

6.3 Minimum requirements for providers

A key means of managing the risks associated with the TIBER-EU test is to use the most competent, qualified and skilled TI and RT providers with the requisite experience to conduct such tests. Consequently, prior to engagement the entity must ensure that the TI and RT providers meet the minimum requirements, which are set out in the TIBER-EU Services Procurement Guidelines. Where feasible, entities should ensure that the procured providers are accredited and certified by a recognised body as being able to conduct a TIBER-EU test.

6.4 Contracts

The entity should make sure when hiring TI and RT providers that there is 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 with the TI and RT providers should include:

- a requirement for the providers to meet security and confidentiality requirements at least as stringent as those followed by the underlying entity for confidentiality requirements;
- the protection of those involved (e.g. indemnifications);
- a clause related to data destruction requirements and breach notification provisions;
- activities that are not allowed during the test, such as: destruction of equipment; uncontrolled modification of data/programs; jeopardising continuity of critical services; blackmail; threatening or bribing employees; and disclosure of results.

The TIBER-EU Services Procurement Guidelines set out in greater detail agreement checklists for the entity and TI/RT providers to consider and apply when formalising their contractual terms.

6.5 Confidentiality and escalation procedures

Protecting the confidentiality of the test is crucial to its effectiveness. To that end, the entity should limit awareness of the test to a small trusted group whose members have the appropriate levels of seniority to make risk-based decisions regarding the test.

The entity should clearly define which measures are to be taken to ensure that only the WT is informed about the test (e.g. WT members may sign a non-disclosure agreement (NDA) to ensure their confidentiality throughout the test). The WT should also define escalation procedures to avoid the triggering of actions that would be mandatory in the case of a real event. Such actions include communicating with an external party (e.g. declaring an incident to a computer security incident response team, sharing information on a platform, etc.) or calling the police.

6.6 Advance readiness check

Entities should conduct thorough due diligence of in-scope systems prior to any testing to ensure that backup and restoration capabilities are in place.

6.7 Management of risks during the test

Crucially, the entity is responsible for the red team test and should therefore remain in control of the process. The TTM should be closely involved in each TIBER-EU test to ensure that the test proceeds according to the scope, scenario, planning and process agreed and described in the framework documents developed collaboratively.

The WT may at any time order a temporary or complete halt if concerns are raised over damage (or potential damage) to a system. Trusted contacts within the WT positioned at the top of the security incident escalation chain should help to avoid miscommunication and prevent knowledge about the TIBER-EU test from being leaked.

During the process of the test, if the TTM suspects that the BT is aware of the test taking place, and subsequently takes steps to manipulate the integrity of it, the lead authority should invalidate the test and not recognise it as a legitimate TIBER-EU test. Knowledge of any compromise of the test will be apparent through the continuous engagement between the TTM and RT provider.

6.8 Use of code names

Given the sensitive nature of the tests, and the potentially detailed findings on the weaknesses and vulnerabilities of specific entities, all stakeholders must use code names for the entities being tested, rather than explicitly naming the entity. All documentation and multilateral communication should refer to the entity by the commonly agreed code name to protect its identity.

7 Preparation phase

7.1 Overview

During the TIBER-EU preparation phase, the engagement for the TIBER-EU test is formally launched, and the TTM starts liaising with the participating entity. The scope is established and the entity procures the TI and RT providers. This phase lasts approximately four to six weeks, not including the duration of the entity's procurement process. An overview of the key activities involved in this phase is shown in Figure 4.

7.2 Pre-launch

Following the adoption of the TIBER-EU framework at national or European level, each lead authority should decide which entities should be invited to undertake a TIBER-EU test. Once the lead authority and entity agree to undertake this test, the relevant authorities should be identified, the authority responsible for leading the test should inform its TCT – and the TCTs of all other relevant authorities, if this is deemed appropriate – and the parties involved in the TIBER-EU test should be briefed on the TIBER-EU process, documentation, roles and responsibilities.

The pre-launch meeting marks the start of the planned and agreed TIBER-EU test process for each individual entity. The TTM asks the entity to establish a WT. This comprises a select number of individuals who are experts (e.g. cyber, operational and risk specialists, experts from the business areas that support the CFs, etc.) and are positioned at the top of the security incident escalation chain. The composition of the WT can be flexible, depending on the specific structure and organisational set-up of the entity. The WTL makes sure that the WT is aware of the TIBER-EU red team test, the need for secrecy and the process the team should go through in case the BT detects and escalates a TIBER-EU related incident. The WTL holds the pre-launch session with the TTM and any additional WT members that the lead wishes to involve. Further guidance on the WT can be found in the TIBER-EU White Team Guidance.

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

- the TIBER-EU process as reflected in the TIBER-XX Implementation Guide;
- the stakeholder roles and responsibilities;
- the security protocols (including the set-up of secure document transfer);
- contractual considerations (including sharing of documentation from TI/RT providers);

- project planning.

With regard to contractual considerations, the smooth delivery of a TIBER-EU test requires a transparent process with the appropriate information and documentation flowing freely, safely and securely between the relevant parties. To facilitate the free, safe and secure flow of information, participating parties can sign an NDA.

7.3 Procurement

After the pre-launch meeting, the entity should start its procurement process. Owing to the sensitive nature of the red team test, and the fact that it is carried out on the live production systems, it is critical that the external TI and RT providers possess the highest levels of skills, capabilities and qualifications. The entity must therefore select external TI and RT providers with the requisite skills and experience to perform the test.

To ensure that the TI/RT providers meet the appropriate standards for conducting such a test, the entity should procure the services of TI/RT providers that have undergone a formal TIBER-EU certification and accreditation process carried out by an organisation or authority that specialises in this task.

In the absence of such an organisation or authority, the entity should conduct its own due diligence as part of its procurement process and existing risk management practices to ensure that each TI/RT provider meets all the requirements set out in the TIBER-EU Services Procurement Guidelines. However, once EU certification and accreditation capabilities are in place, all entities should rely on these for TIBER-EU test. Responsibility for ensuring that the appropriate TI/RT providers are selected lies solely with the entity.

The TIBER-EU Services Procurement Guidelines set out in detail the minimum requirements for TI/RT providers. These are deliberately stringent requirements intended to mitigate the risk of tests being conducted by inexperienced personnel, which could have an adverse impact on the entity.

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

- draw on best practice procurement guidelines to identify potential TI/RT providers capable of meeting the objectives of the test;
- issue an invitation to tender in compliance with the TIBER-EU framework and any relevant procurement legislation;
- assess tender responses, and then interview and select appropriate providers;
- establish conditions governing the sharing, confidentiality and retention of intellectual property rights.

Once the procurement process has been completed and all relevant contractual arrangements are in place, the entity should complete the TIBER-EU Test Project

Plan, including the final schedule of meetings to be held between the entity, TI/RT providers and TCT, and share this with all the relevant stakeholders.

Entities may apply a degree of flexibility on the timing of the procurement, as the process may differ across jurisdictions. Hence, the lead authority's TCT should exercise a degree of judgement over whether to allow the entity 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. The entity should, as early as possible, develop a draft TIBER-EU Test Project Plan taking into consideration timelines, procurement, etc. to ensure that there are no bottlenecks or delays in the overall testing process.

7.4 Launch

Since cooperation is key for a successful TIBER-EU test, the launch meeting is a physical meeting that should involve all the relevant stakeholders (including the TTM, WT and TI/RT providers). During this meeting, all stakeholders discuss the test process and their expectations, as well as the draft TIBER-EU Project Plan, which should be prepared by the WT.

7.5 Scoping

The key objective of scoping is for the entity and the relevant authorities to agree the scope of the red team test. The scope must include the entity's CFs. 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.

Within the TIBER-EU framework CFs are defined as:

"the people, processes and technologies required by the entity to deliver a core service which, if disrupted, could have a detrimental impact on financial stability, the entity's safety and soundness, the entity's customer base or the entity's market conduct".

Note that a CF is not a system. It is a function which could be considered critical or essential to the financial services sector and/or a financial services sector organisation. Entities across the sector support and deliver these functions in different ways via their own internal processes, which are in turn underpinned by critical technological systems. It is these critical technological systems, processes, and the people surrounding them that are the focus of TIBER-EU threat intelligence and red team testing. In most cases, this will also include the systems, people and business processes underpinning the entity's CFs that are outsourced to third-party service providers.

For the purposes of a TIBER-EU test, testing must be performed on the live production systems of the entity. However, the entity may also include other types of

infrastructure, including pre-production, testing, backup and recovery systems, within the scope of the red team test.

The purpose of scoping is for all relevant parties, i.e. the TCT and entity, to agree on the scope of the test and the identification of the CFs. Both the TCT and entity should have extensive knowledge of the entity's business model, functions and services.

Entities may conduct a business impact analysis defining the CFs as part of their standard operational risk management practices. In defining the CFs and consequently the scope of the test, the entity may also refer to the Generic Threat Landscape Report (GTL Report) to further contextualise its business and the threats it faces, and to map the possible threat scenarios to its CFs. The GTL Report is discussed in more detail in Chapter 8.

7.6 Setting and capturing the flags

During the scoping process, the entity must complete a TIBER-EU Scope Specification document. The TIBER-EU Scope Specification sets out the scope of the TIBER-EU test, and lists the key systems and services that underpin each CF. This information helps the WT set the "flags" to be captured, which are essentially the targets and objectives that the RT providers must strive to achieve during the test, using a variety of techniques.

The WT should discuss the flags with the TTM, who must approve them. Although the flags are set during the scoping process, they can be changed on an iterative basis following the threat intelligence gathering and as the red team test evolves.

7.7 Scoping meeting

The final TIBER-EU Scope Specification document should be agreed by the TTM during a workshop organised by the entity for all relevant stakeholders (i.e. WT, TTM and possibly the TI/RT providers). Importantly, the scope will need to be agreed at the board level of the entity.

If the procurement has been completed, the scoping process and meeting may include the TI/RT providers. Alternatively, the entity may opt to exclude the TI/RT providers at this stage. In any case, it is recommended that the WT and TTM discuss this in advance of the scoping meeting.

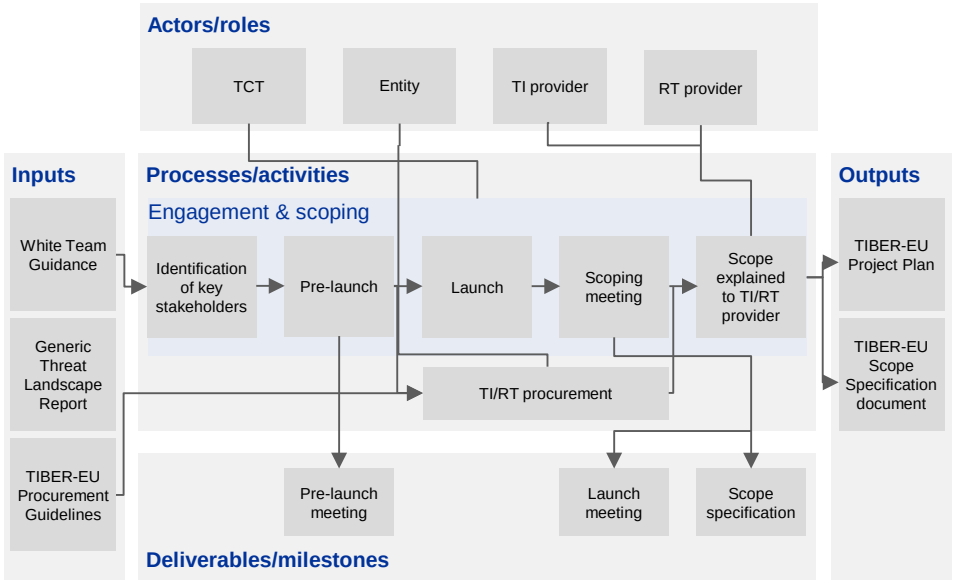
7.8 Explanation of the scope to the TI/RT providers

For the test to be successful it is important that the TI/RT providers understand the business of the entity. Therefore, if the TI/RT providers are not already involved during the scoping process, a meeting should be planned with the providers after the

scoping process to explain the CFs and systems underpinning them. If the entity feels that further dialogue on the functioning of its business is necessary to arrive at realistic scenarios, the TIBER-EU framework encourages this. The sharing of knowledge between the entity and TI/RT providers will facilitate a smooth transition to the next phase of target intelligence gathering.

Figure 4

Overview of the TIBER-EU preparation phase



8 Testing phase: threat intelligence and scenarios

8.1 Overview

Once the scope has been agreed, the TI/RT providers have been contracted, and all parties have been informed of their roles and responsibilities, the testing phase should commence, with threat intelligence a key component. Threat intelligence-based scenarios mimicking real-life cyber adversaries are essential to the success of testing activities. There are two complementary tools to develop these threat intelligence-based scenarios: the GTL Report and the TTI Report. The duration of the targeted threat intelligence process in this phase is approximately five weeks.

The GTL Report should reflect the most significant threats faced by the financial sector, whether at a national or European level. The GTL Report can be used to develop the TTI Report, which gives a more detailed view of the specific entity's current defences and attack surface and helps produce actionable and realistic attack scenarios. Such attack scenarios look to emulate the TTPs of real-life threat actors within a threat landscape and will be used to deliver a realistic simulation. These scenarios will be integrated into the RT provider's Red Team Test Plan and help the RT provider to deliver a practical assessment of the entity's defensive security controls, and its detection and response capabilities.

8.2 Generic threat landscape

Given the critical role of threat intelligence to a TIBER-EU test, entities must procure a TTI Report, which sets out the specific threat scenarios they may be faced with. The scenarios will allow the RT provider to conduct a realistic and meaningful test. However, the TIBER-EU framework recommends that national jurisdictions first produce a national GTL Report for the financial sector to complement the more specific TTI Report.

The GTL Report should elaborate on the specific threat landscape of the country, taking into consideration the geopolitical and criminal threats unique to the jurisdiction. The report should consider key financial market participants and their CFs, including (wholesale and retail) banks, broker-dealers, financial market infrastructures, financial market utilities, and other critical third parties, the different threat actors (including their TTPs) targeting these entities, and the common vulnerabilities. The GTL Report is used to define the specific threat actors targeting the different types of entities, complements the production of the TTI Report and provides the basis for later scenario development. If produced at an early stage of the process, the GTL Report should also be used during the preparation phase to guide and inform the initial scoping discussions with the entity.

The GTL Report will allow TI providers to:

- help translate the information contained in the GTL Report into specific strategic, operational and tactical threat intelligence that is relevant to the entity;
- focus their efforts on more detailed reconnaissance to provide the RT provider with more bespoke and specific information on the entity, which will in turn allow meaningful attack scenarios to be developed and a more effective test to be performed.

The GTL Report aims to provide TI providers with a solid base of information and analysis, which can then be used to produce more entity-specific TTI Reports. Although a GTL Report is not mandatory, it can be more cost-effective for the financial sector in each jurisdiction to produce one, with each TI provider and entity using it as a common tool when developing the more specific TTI Reports.

8.3 Production and ownership of the GTL Report

The GTL Report may be instigated and produced by the authority, the market (e.g. industry bodies, a consortium of entities or any other financial sector body), or both in partnership. The report may also be produced by external providers. In any case, it is recommended that the report be shared more widely with the financial sector. To provide a broad and realistic overview of the threat to the national (and possibly European) financial sector, the GTL Report should be developed using appropriate financial sector threat intelligence expertise. Appropriate threat intelligence expertise can be sourced from entities, national authorities, commercial TI providers, information sharing and analysis centres (ISACs), market associations and government agencies.

As the threat landscape is constantly evolving, the GTL Report should be updated on an ongoing basis as new threat actors, TTPs and vulnerabilities enter the landscape. Updates should be carried out at least annually.

The TI provider should connect the GTL Report to the TTI Report (explained in more detail below) to develop specific threat scenarios for the targeted entity. The RT provider should be consulted to ensure the scenarios are actionable.

8.4 Governmental intelligence

If possible, at national level the GTL Report should be offered to the national intelligence agency – and any other relevant governmental agencies[6] – for feedback and further enrichment, and ideally for validation.

[6] For example, the national cyber security centre, national high-tech crime unit, general intelligence agency and military intelligence agency.

In some cases, the GTL Report may also be shared with the European Union Agency for Network and Information Security (ENISA) for feedback and enhancement. If it is not feasible for national intelligence agencies or any other relevant governmental agencies to provide feedback on the report, authorities may seek to consult with a financial sector group with expertise in threat intelligence.

8.5 Targeted threat intelligence process

The targeted threat intelligence process results in the production of a TTI Report, which is a bespoke, focused threat intelligence report for the entity being tested. Its aim is to use specific targeted threat intelligence and reconnaissance related to the entity, taking into consideration the real-life actors within the threat landscape, to help develop attack scenarios. Responsibility for the development and production of the TTI Report lies with the TI provider. The RT provider[7] becomes involved towards the end of the phase when it absorbs the contents of the TTI Report and integrates the attack scenarios into a Red Team Test Plan.

The TIBER-EU process is designed to create realistic threat scenarios describing attacks against an entity. These scenarios can be used by a simulated attack team to guide its red team test. The scenarios are based on available evidence of real-world threat actors, combined with OSINT data on the entity as well as some knowledge of the CFs that form the scope and target of the red team test.

While this approach is highly valuable, real-world threat actors may have months to prepare an attack. In addition, while TI providers are constrained by limitations on the time and resources available, and by moral, ethical and legal boundaries, real-word threat actors are free of such constraints. This difference can cause difficulties when attempting to create realistic scenarios, as knowledge about the internal network is often the hardest to gain using morally, ethically or legally justifiable techniques.

Similar constraints apply to CFs, which are, by their nature, internal to the entity and so typically do not have a large footprint in the public domain. They also apply to the systems that underpin CFs, whether these are bespoke internal systems or external systems that span multiple organisations with a common connecting infrastructure.

Therefore, to make intelligence gathering as efficient as possible given the time and resource constraints, and to ensure the intelligence is relevant to the scope and the entity's business, the TI provider should seek from the entity and be provided with:

- a business and technical overview of each CF-supporting system in scope;
- the current threat assessment and/or threat register;
- examples of recent attacks.

[7] It should be noted that some providers provide both TI and RT services, and entities can opt to procure such services from these providers.

The entity should provide the above information to the TI provider in the “Input for the Targeted Threat Intelligence” template.

In cases where the entity has an internal threat intelligence capability or function, the TI provider should liaise with it and gather relevant information that will help inform the TTI Report.

Finally, in cases where the national jurisdiction has produced a GTL Report, the TI provider should use this as a basis for producing the TTI Report, focusing on how to adapt the threat landscape of the country, the different threat actors and the common vulnerabilities to the specificities of the entity.

8.6 Elements of the targeted threat intelligence process

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

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

Information gathered from targeting and threat intelligence, in part provided through the Input for the Targeted Threat Intelligence template, should be used to facilitate scenario development (see Section 8.10 below).

8.7 Target identification

To identify targets, the TI provider should carry out a broad exercise of the kind typically undertaken by threat actors as they prepare for their attack from outside the network. The objective is to form a detailed preliminary picture of the entity and its weak points from the attacker’s perspective. This will enable the threat intelligence to be put into context and will contribute to the development of the threat scenarios in the TTI Report. Part of this information should be provided by the entity using the Input for the Targeted Threat Intelligence template.

The output of this activity is the identification, on a CF-focused, system-by-system basis, of the attack surfaces of people, processes and technologies relating to the entity, and its global digital footprint. This includes information that is intentionally published by the entity and internal information that has been unintentionally leaked. Such information could be customer data, confidential material or other information that could prove to be a useful resource for an attacker.

Targeting represents a valuable input and is a core element of the TTI Report, where it is used to tailor the threat profile and scenarios. By revealing some of the entity’s attack surfaces and identifying initial targets, it also serves as a valuable input into the RT provider’s deeper and more focused targeting activities.

8.8 Threat identification

With regard to threats, the TI provider collects, analyses and disseminates intelligence about relevant threat actors and probable threat scenarios. The objective is to present a credible picture of the cyber threat landscape, based on evidence-backed threat intelligence which is specifically tailored to the entity's business environment. In cases where a GTL Report has been produced, the TI provider can use it to further complement the identification of threats.

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

As mentioned above, this part of the report builds on intelligence acquired during the target identification process. For example, any relevant assets identified (such as an exposed insecure server) will be integrated into scenarios so the RT provider can exploit them. While the ultimate goal is to find intelligence directly relating to the CFs in scope, these CFs are by their nature buried within the entity's organisation. In addition, while CF-specific intelligence evidence may not always be discoverable, the TI provider may find evidence of a more general threat that applies to one or more CFs.

While the threat scenarios in this report are fictional, they are based on real-life examples of cyber attacks including the motivations of the attackers, their objectives, and the methods they employ to meet them. By focusing on what is probable rather than theoretically possible, the threat identification part of the TTI Report supports the RT provider in justifying the approach it plans to take.

8.9 Targeted Threat Intelligence Report

Equipped with the output from target identification and threat identification, which make up the TTI Report, the TI and RT providers will have a firm evidential basis for the proposed red team test, which include the attack scenarios. Three outputs are particularly relevant in this respect:

- tailored scenarios, which will support the formulation of a realistic and effective Red Team Test Plan;
- threat actor goals and motivations, which will help steer 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.

The TI provider should complete the TTI Report and then share it with the entity, the TTM and the RT provider. A thorough review should be undertaken, with any factual errors corrected and any issues discussed.

In addition, based on the TTI Report, the WT and TTM may opt to update or modify the flags.

8.10 Scenario development

Scenario development represents the key transition point between the TI and RT providers. This activity takes place either just before or in parallel with the national intelligence agency evaluation (where applicable) of the TTI Report (see Section 8.11 below).

Using the scenarios contained in the TTI Report, and in line with the TIBER-EU Test Scope Specification, the RT provider should develop and integrate the attack scenarios into a draft Red Team Test Plan. At this stage, a workshop may be held, involving the entity, TTM and TI/RT providers, during which the TI provider goes through the scenarios and the RT provider goes through the draft Red Team Test Plan (see Section 8.11 below).

8.11 Intelligence feedback

Where possible, jurisdictions may seek feedback on the TTI Report from their respective national intelligence agencies or other governmental agencies, such as the national cyber security centre, national high-tech crime unit, military intelligence agency, etc. During the intelligence feedback process, the relevant agencies should review the draft versions of the TTI Report and liaise directly with the TTM with any comments and enhancements.

After the intelligence feedback process, a threat intelligence/scenario workshop must be held involving all relevant stakeholders, namely the entity's WT, the TTM (and possibly the supervisor and/or overseer) and the TI/RT providers. The workshop activities are as follows:

- the TI provider presents an overview of the TTI Report and summarises the proposed changes to the reports following feedback from the national intelligence agency and/or other agencies;
- the TTM provides feedback comments on the TTI Report;
- the RT provider presents the draft Red Team Test Plan, including CF scenario mapping, flags, possible anticipated leg-ups[8], risk mitigation, escalation procedures, test start/stop dates and a draft Red Team Test Report delivery date.

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

Following the workshop, the TI provider should revise and produce a final version of the TTI Report for delivery to the entity.

In addition, the RT provider should revise the draft Red Team Test Plan in the light of the workshop findings and the risks identified.

8.12 Key considerations for the TI provider

For the TIBER-EU framework to work effectively, it is critical that the targeted threat intelligence process and subsequent deliverables meet the highest standards. Intelligence encompasses not only the technical details of the attack but also an understanding of the TTPs behind the attack and the attackers themselves.

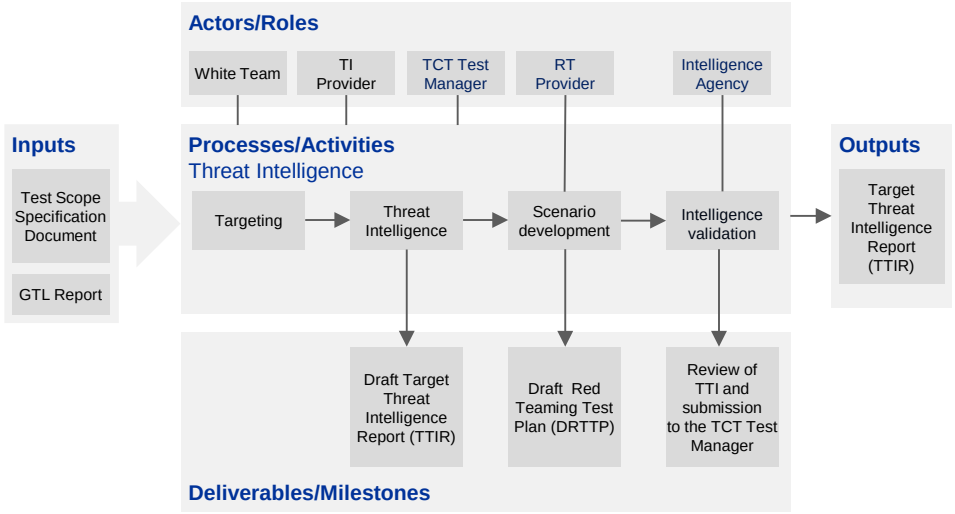
During the process of producing the TTI Report, the TI provider should take into consideration a number of factors.

- TI providers must engage with the entity to obtain useful context for conducting the threat analysis. Although the entity may not always be able to share the details of sensitive incidents with the TI provider, it should still be possible to learn about the entity both through engagement with the key stakeholders and by gathering evidence of previous breaches through public sources.
- TI providers should use a broad range of sources (e.g. internet services, a mixture of public and private fora and a range of media types such as internet relay chats, email and video). The number of items in any given source type is again a useful means of measuring the likely catchment capability of any collection function. However, volume can at times undermine quality, and it is expected that the collection of sources be balanced against the ability of the TI provider to refine, analyse and discard sources in an accurate manner.
- TI providers should have a depth of sources. TI providers collecting intelligence may only use surface content from a given source, but it is also important to know that all the content of a given source can be incorporated when there is an appropriate and lawful opportunity to do so. It is therefore expected that a TI provider can provide the option to acquire data at scale and in its original context.
- TI providers should have adequate language support. Languages play an important role in providing cyber threat intelligence. Cyber threats are a global phenomenon, and a TI provider that offers little linguistic coverage of online threats will potentially miss a significant proportion of relevant information.
- TI providers should be able to use a variety of methods in intelligence gathering, for example OSINT (which is derived overtly from publicly available sources) and HUMINT (human intelligence, which is derived overtly or covertly from human sources).
- TI providers must always demonstrate strong ethical behaviour.

- TI and RT providers must work together in a collaborative, transparent and flexible manner. A TI provider must demonstrate willingness and the ability to work in this way, sharing its deliverables with its RT counterpart for review and comment. The TI provider should also demonstrate a willingness to work with the RT provider during the remainder of the TIBER-EU test. This includes the creation of testing scenarios, as well as any new intelligence requirements that occur as the red team test progresses. The TI provider is expected to provide input into the final report issued to the entity.

Figure 5

TIBER-EU testing phase – overview of threat intelligence and scenarios



9 Testing phase: red team testing

9.1 Overview

Following completion of the targeted threat intelligence process, the RT provider takes the lead. During the red team testing phase, the RT provider plans and executes a TIBER-EU intelligence-led red team test of the target systems and services that underpin each CF in scope. This is followed by a review of the test and issues arising.

It is important that sufficient time be allocated to the red team testing phase to allow the RT provider to conduct a realistic and comprehensive test in which all attack phases are executed and all test objectives are achieved. The test objectives (i.e. compromise actions) agreed during the scoping phase (and possibly updated during the targeted threat intelligence process) are the flags that the RT provider must attempt to capture during the test as it progresses through the scenarios.

The time allocated for testing should be determined by the scope, the entity's resources, any external requirements for a given engagement, and the availability of supporting information supplied by the entity (e.g. regular vulnerability reports or previous assessment data). In general, the time allocated to testing should be proportionate to the scope, although based on experience it is envisaged that 10–12 weeks would be a reasonable amount of time for testing.

9.2 Testing methodology

The RT provider should deploy a range of TTPs during the test. The following is just one example of a testing methodology that the RT provider may use.

Reconnaissance – The first phase in a red team test is focused on collecting as much information as possible about the target. Reconnaissance is one of the most critical steps, and it is usually possible to learn a great deal about the target's people, technology, surroundings and environment. This step may also involve building or acquiring specific tools for the engagement. Reconnaissance should primarily be undertaken by the TI provider, although the RT provider will also take part in this activity during the build up to the test.

Weaponisation – Another important phase in a red team test involves analysing the information gathered about the infrastructure, facilities and employees. By means of this thorough analysis, the red team begins to form a picture of the target and its primary operations. Effective weaponisation involves preparation for the operations specific to the targets.

Delivery – This is a critical stage of the execution phase and marks the active launch of the full operation. The red team begins to carry out the actions on the target(s) intended to reach the targets or flags, such as social engineering, analysing

cyber vulnerabilities, planting hardware trojans for remote network persistence, etc. One of the most important objectives is to identify the best opportunities for exploitation.

Exploitation – During exploitation, the red team's goal is to "break in", i.e. to compromise servers/apps/networks and exploit target staff through social engineering. The exploitation stage paves the way for the control and movement phase.

Control and movement – Once a successful compromise has been performed, attempts to move from initial compromised systems to further vulnerable or high-value systems will be made. For example, this may consist of "hopping" between internal systems, continually reusing any increased access obtained in order to eventually compromise agreed target systems.

Actions on target – This entails gaining further access to compromised systems and acquiring access to previously agreed target information and data. At this point, the red team aims to complete the test and achieve the objectives agreed upon and set by the entity during the scoping and threat intelligence processes.

9.3 Red Team Test Plan

Prior to the commencement of the test, the TI provider must have a handover session with the RT provider, providing a detailed explanation of the TTI Report and discussing possible threat scenarios for the testing. The RT provider should gain insight from this handover meeting and further review the TIBER-EU Scope Specification, the GTL Report (if produced) and the TTI Report to finalise the Red Team Test Plan. This information and documentation provides the evidential basis for designing and justifying the proposed Red Team Test Plan and attack scenarios.

The RT provider should align its test objectives with the goals of each of the actors, map these to the CF-supporting systems, and produce credible real-life attack scenarios for the test. The attack scenarios are designed to provide background to the tradecraft employed by each threat to conduct a successful attack. The RT provider should therefore adapt its attack methodology to replicate the real-life attack scenarios.

The RT provider should additionally draw upon the TTI Report, which reveals some of the entity's attack surfaces, as a basis for deeper and more focused targeting activities.

The RT provider could also add some elements which test the response of the entity, including evidence on whether the compromise action would be immediately detected or could have a fair chance of succeeding.

Performing any sort of red team test always carries a level of risk to the target system and the business information associated with it. Risks to the entity, such as degradation of service or disclosure of sensitive information, need to be kept to an

absolute minimum. The RT provider should therefore include an appropriate plan for managing these risks.

The output of this activity is the final Red Team Test Plan, including the attack scenarios to be followed and the risk management controls that will be applied to ensure that the test is conducted in a controlled manner.

9.4 Scenarios

The attack scenarios are written from the attacker's point of view and should define the concrete targets to be reached (i.e. the flags to be captured). The RT provider should indicate various creative options in 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 scenario writing is a creative process. The TTPs do not simply mimic scenarios seen in the past, but combine the techniques of the various relevant threat actors.

In some cases, the implementation of the framework (TIBER-XX) may also include using TTPs which look to breach the physical security of the entity to gain access to the network or plant a device. However, if such a method is adopted as part of the TIBER-XX implementation, appropriate safeguards (e.g. formal consent by the entity) should be in place and no legal boundaries should be crossed.

In addition to these scenarios, an RT provider may develop other types of scenarios. In many cases, the use of conventional TTPs may not be successful in achieving a target; to emulate a real-life attacker in such a case, the RT provider could deploy creative and innovative TTPs, stretching itself to its absolute limits. The RT provider can leverage its full range of professional knowledge, research, expertise and tools to build forward-looking scenarios based on TTPs that have not yet been seen but are expected in the future.

9.5 Additional information from the entity and TI provider

The TIBER-EU process is designed to create realistic scenarios mimicking possible future attacks against the entity. Real-world threat actors may have months to prepare an attack. They are also able to operate freely without the constraints that TI/RT providers face, such those on time and resources – not to mention the moral, ethical and legal boundaries. This difference can cause challenges when attempting to create realistic scenarios, as knowledge about the internal network is often the hardest to gain using morally, ethically or legally justified techniques.

Similar constraints apply to the systems underpinning the CFs, which 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 a common connecting infrastructure, the RT provider's knowledge of the functioning of these

systems may be limited in comparison with that of attackers who have the capacity and time to study them extensively.

Therefore, to facilitate a more effective and efficient test, the entity may deliver additional information to the RT provider on the scenarios chosen, including on the people, processes and systems targeted in the scenario. This information may give the RT provider further insights and allow a better use of time. However, it is up to the entity to provide this additional information and the underlying level of detail at its discretion.

If the entity provides additional information, the TIBER-EU test will reflect a “grey box” testing approach in contrast with the “black box” approach. Experience shows that the more relevant information an entity gives to the RT provider, the more the participating entity will gain from the test. However, it should be evident that the information given to the RT provider could have been obtained by an advanced attacker with more time and unhindered by moral, ethical and legal constraints.

In addition to the information provided by the entity, the role of the TI provider can be enhanced during the testing phase. For the test to succeed, the TI provider can provide ongoing threat intelligence to the RT provider during the test, which may provide more useful reconnaissance and more insight on how to achieve the targets. In real life, the attacker can leverage threat intelligence while attempting to compromise an entity. Allowing a fluid relationship between the TI and RT providers during the test may add greater value to the entity. Where TI and RT providers decide to work more closely during the test, the working arrangements and information sharing arrangements must be agreed between the two parties.

9.6 Execution of the test

During the execution of the test, the RT provider should perform a stealthy intelligence-led red team test of the target systems. The attack scenarios are not a prescriptive playbook which must be followed precisely during the test. If obstacles occur, the RT provider should show its creativity (as advanced attackers would) to develop alternative ways to reach the test objective or flag.

RT providers are constrained by the time and resources available as well as by moral, ethical and legal boundaries. It is therefore possible that the RT provider may require occasional leg-ups from the WT to help them progress. During the testing phase, the RT provider may be unable to progress to the next stage owing to time constraints or because the entity has been successful in protecting itself. In such scenarios, the RT provider, with agreement from the WT and TTM, may be given a leg-up, where the entity essentially gives the RT provider access to its system, internal network, etc. to continue with the test and focus on the next flag/target. Should this happen, then the leg-up should be duly logged. This ensures that maximum benefit is derived by all stakeholders from a time-limited test.

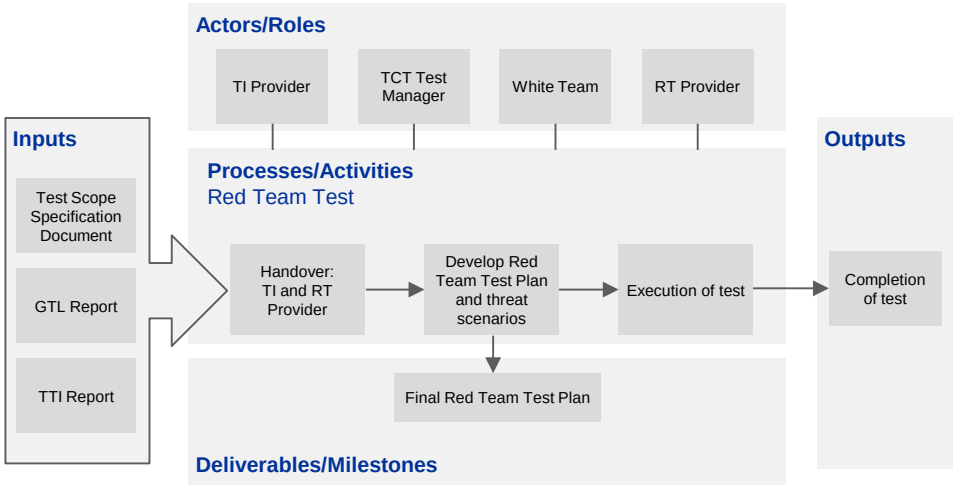
The TTM should be updated at least once a week by the RT provider, while the WT should be kept abreast of progress on an ongoing basis. If feasible, physical

meetings between the WT, TTM and RT provider during this phase are strongly encouraged, since the discussions add significantly to the quality of the test and help build a relationship of trust. However, any such meeting should be conducted cautiously to ensure that the BT is not made aware of the ongoing test.

Irrespective 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 bring risks to the entity and its CFs. It is important for the WT and TTM to be continuously informed 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 achieved the “capture the flag” moment. These updates provide the WT with the opportunity to discuss with the RT provider and TTM what actions can and cannot be taken next. It also provides a chance for escalation procedures to be invoked where necessary. The WT can halt the test at any time if it considers it necessary to do so. 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.

Figure 6

TIBER-EU testing phase – overview of the red team test



10 Closure phase

10.1 Overview

The closure phase (which includes remediation planning and result sharing) allows all relevant stakeholders to reflect on the outcome of the test and make improvements to further enhance the cyber resilience of the entity. In this phase, the RT provider will draft a Red Team Test Report, which will include details of the approach taken to the testing and the findings and observations from the test.

Where necessary, the report will include advice on areas for improvement in terms of technical controls, policies and procedures, and education and awareness; the relevant stakeholders will replay the executed scenarios and discuss the issues uncovered during the test; the entity will take on board the findings, and agree and finalise a Remediation Plan (including planning for follow-up testing) with the authorities; the process will be reviewed, and the entity's detection and response capabilities assessed and discussed; and the key findings from the test will be shared with other relevant authorities. The duration of the close-down activities in this final phase is approximately four weeks.

10.2 Red Team Test Report and Blue Team Report

The output of this activity is a draft version of the Red Team Test Report produced by the RT provider for delivery to the entity, which then forwards the document to the TCT. The draft report must be issued within two weeks of test completion. The key members of the entity's BT are informed of the test and will use the Red Team Test Report to deliver their own Blue Team Report. In the Blue Team Report, the BT maps its actions alongside the Red Team's actions. The Blue Team Report should be completed ahead of the replay workshop (see Section 10.3 below) to maximise the learnings from the replay.

10.3 Red Team and Blue Team replay

After the RT provider and BT deliver their reports, the entity must arrange a replay workshop. The goal of this workshop is to learn from the testing experience in collaboration with the RT provider. During the workshop, a replay is organised in which the BT and the RT provider review the steps taken by both parties during the test.

Additionally, a purple teaming element can be added, in which the BT and the RT provider 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.

When conducting the replay, the RT provider should state how well the testing team managed to progress through the targeted attack life cycle stages of each scenario. The RT provider should also offer an opinion as to what else could have been achieved with more time and resources given that genuine threat actors are not constrained by the time and resource limitations of TIBER-EU.

The TTM and TI provider can also be present during these replay workshops.

10.4 360-degree feedback

During the 360-degree feedback meeting, the entity, TCT, and (TI and) RT providers should come together to review the TIBER-EU test. The TCT should arrange and facilitate the workshop. In the 360-degree feedback meeting, all parties should deliver feedback on each other and on the overall process. The goal is to further facilitate the learning experience of all those involved in the process for future exercises. The key topics to be covered, from all parties' perspectives, are:

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

In this way, the TI and RT providers will obtain feedback on their performance, and the relevant authorities will have opportunities to identify and improve the TIBER-EU process.

The TCT may share the output from the 360-degree feedback on an anonymous basis with the TKC so that all lessons learned can be reflected on and improvements can be made to the TIBER-EU framework. This is a key part of the "learning and evolving" principle that underlies the TIBER-EU framework.

10.5 Remediation Plan and Test Summary Report

After the BT and RT provider replay and the 360-degree feedback workshop, the entity should draft its Remediation Plan and Test Summary Report.

The Remediation Plan is based on the test results, which should be used in turn to support the business case for implementing improvements to mitigate the vulnerabilities identified during the TIBER-EU test.

The Test Summary Report summarises the overall test process and results (including the Remediation Plan) and should draw on the test documentation, such as the Red Team Test Report, the Blue Team Report, the TTI Report, the Red Team

Test Plan and the Remediation Plan. The Test Summary Report should not contain detailed technical information and findings regarding weaknesses and vulnerabilities, as information at that level of detail is highly sensitive and for the entity only. The entity must share the Test Summary Report with the lead authority. The lead authority may also review the more detailed findings from the test if this is deemed necessary.

10.6 Confirmation and result sharing

At the end of the test, once the reports and Remediation Plan have been agreed, the entity, TI/RT providers and lead authority should provide an attestation confirming that the test was conducted in accordance with the core requirements of the TIBER-EU framework. The attestation should be signed by the board of the entity and TI/RT providers, and can serve as a means of qualifying the test for mutual recognition among other relevant authorities.

In cases where the other relevant authorities did not participate in the test but there was mutual agreement to share the test results, the lead authority and entity should share the Test Summary Report and attestation. The Test Summary Report serves as a form of assurance to other relevant authorities, and the attestation qualifies the test as a legitimate TIBER-EU test.

As one of the key objectives of the TIBER-EU framework is to enhance sector resilience, the TCT of each jurisdiction should analyse the results of all the tests to identify the key findings, common threats and vulnerabilities, and to disseminate these in the appropriate form to relevant stakeholders. The TCT may also share anonymised findings or lessons from their respective TIBER tests with the TKC. This information will allow the TKC to aggregate the key findings, common threats and vulnerabilities, to form a picture 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.

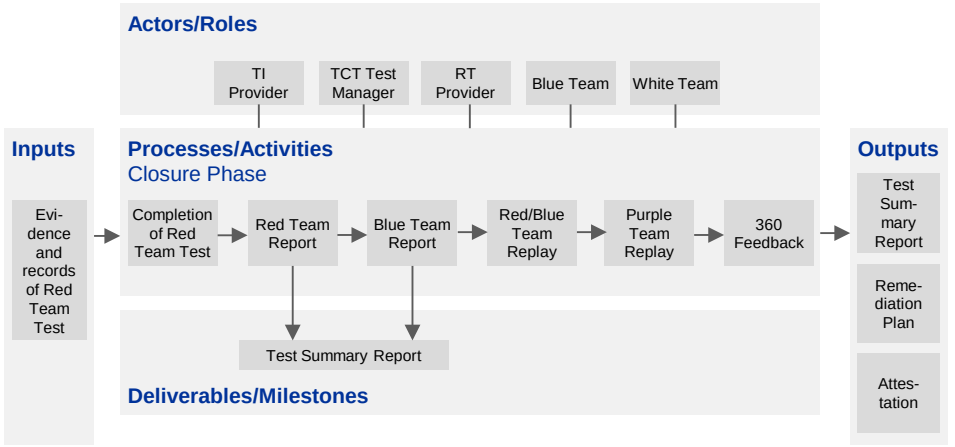
10.7 Oversight and supervision

From the outset, it is up to the relevant authority to determine the role of the overseer and supervisor in the TIBER-XX implementation. In some cases, the authority may opt to include the overseer and supervisor throughout the entire testing process, while in some jurisdictions the authority may opt to formally exclude the involvement of the overseer and supervisor.

In cases where the overseer and supervisor have not been involved during the testing phase, the TCT should notify the oversight and supervisory functions once the test has ended. At this stage, it is recommended that the overseer and supervisor work with the entity to implement the remediation measures.

Figure 7

Overview of the TIBER-EU closure phase



11 Annex

11.1 TIBER-EU requirements

Table 1

Adoption and implementation

Requirements	Mandatory	Optional
The TIBER-EU framework is adopted and implemented by each jurisdiction in the EU.		✓
If a jurisdiction decides to implement a TIBER-XX framework, then the framework is formally adopted by an authority, and the TIBER-EU Knowledge Centre is informed.	✓	
The jurisdiction adopts the TIBER-XX framework as a supervisory or oversight tool, as a catalyst, or for the purposes of financial stability.	✓	
On adoption, the core documentation of the national TIBER-XX framework is published, and the sector is informed.	✓	
The jurisdiction determines which entities should undertake a test – either on a voluntary or mandatory basis.	✓	
The jurisdiction conducts a legal analysis of its TIBER-XX framework to ensure it complies with national laws and regulations.	✓	
The jurisdiction puts in place appropriate governance structures and allocates adequate resources to implement the TIBER-XX framework.	✓	
The jurisdiction has a centralised TIBER Cyber Team (TCT) to manage the programme, oversee the tests and liaise with the TIBER-EU Knowledge Centre.	✓	
In case of cross-border entities, the test is initiated and driven by the lead authority. If another relevant authority seeks to initiate and lead the test, the lead authority must agree to it.	✓	
In case of cross-border entities, the test is conducted jointly between the lead authority and other relevant authorities.		✓
The TIBER-EU test is conducted by independent third-party providers, i.e. external threat intelligence (TI) and red team (RT) providers.	✓	

Table 2

Preparation phase

Requirements	Mandatory	Optional
For each test, there is a White Team (WT), independent TCT (and Test Manager), and external TI/RT providers.	✓	
The national intelligence agency/national cyber security centre/high-tech crime unit is involved in each test.		✓
Once the procurement process has been completed, there are appropriate contracts in place between the different stakeholders, with relevant controls embedded into the contracts, to facilitate a controlled test (in a discreet manner).	✓	
Prior to conducting the test, the WT conducts a risk assessment and then puts in place all the necessary risk management controls, processes and procedures to facilitate a controlled test.	✓	
Throughout the end-to-end test process, in all documentation and communication between stakeholders a code name is used to conceal the identity of the entity being tested.	✓	
At the outset of the test process, there is a launch meeting which includes the WT and TCT.	✓	
The launch meeting also includes other relevant authorities and the TI/RT providers.		✓
The scope of the test includes critical functions (CFs), as well as the people, processes, and technology and databases that support the delivery of CFs. This is documented in the TIBER-EU Scope Specification document and signed off in the attestation by the board.	✓	
The entity expands the scope of the test beyond the CFs and includes other functions and processes.		✓
During the scoping phase, the WT (with agreement from the TCT), sets “flags”, which are targets or objectives, that the RT provider aims to meet during the test.	✓	
The test is conducted on live production systems.	✓	
Only the WT and TCT are informed about the test, its details and the timings – all other staff members (i.e. Blue Team, BT) remain unaware of the test.	✓	
Only TI/RT providers that meet the minimum requirements set out in the TIBER-EU Services Procurement Guidelines can undertake the TIBER-EU test. The TI/RT providers will be TIBER-EU-certified and accredited once the EU has these capabilities in place.	✓	

Table 3

Threat intelligence and red team testing phase

Requirements	Mandatory	Optional
For each test, an external TI provider produces a dedicated Targeted Threat Intelligence Report (TTI Report) on the entity being tested. Where infrastructure has been outsourced and a third party is included in the scope of the test, the TTI Report also includes information about that third party.	✓	
For each national implementation, a Generic Threat Landscape Report (GTL Report) for the country's financial sector is produced and maintained, and is used to help inform the TTI Report.		✓
For each threat intelligence report (TTI and GTL), the national intelligence agency/national cyber security centre/high-tech crime unit is involved to provide feedback.		✓
For each TTI Report on the entity, the TI provider sets out multiple threat scenarios which can be used by the RT provider.	✓	
The TI provider holds a handover session with the RT provider, providing the basis for the threat scenarios.	✓	
Following the handover, the TI provider continues to be engaged during the testing phase and provides additional up-to-date, credible threat intelligence to the RT provider, where needed.		✓
The RT provider develops multiple attack scenarios, based on the TTI Report. This is documented in the Red Team Test Plan and shared with the WT and TCT.	✓	
The jurisdiction, in its implementation of the TIBER framework, allows physical red teaming in the scope of the methodology for the TIBER test (e.g. planting a device at the entity), provided all necessary precautions are taken.		✓
The RT provider executes the attack based on the scenarios (with some flexibility) in the Red Team Test Plan and goes through each of the phases of the kill chain methodology. Where needed, a "leg-up" will be provided by the entity.	✓	
During the test, the RT provider keeps the WT and TCT informed about progress, "capture the flag" moments, the possible need for leg-ups, etc. The RT provider takes a stage-by-stage approach and consults the WT and TCT at all critical points to ensure a controlled test.	✓	
The duration of the red team test is proportionate to the scope, size of the entity, complexity of threat scenarios, etc. Sufficient time is allocated to testing to guarantee that a comprehensive test has been conducted across the enterprise. Experience suggests that a period of at least 10–12 weeks is required.	✓	

Table 4

Closure phase

Requirements	Mandatory	Optional
At the end of the test, the RT provider produces a Red Team Test Report, outlining the findings from the test.	✓	
The entity's BT is informed of the test and uses the Red Team Test Report to deliver its own Blue Team Report. In the Blue Team Report, the BT maps its actions alongside the RT provider's Team actions.	✓	
At the end of the test, the RT provider, the BT and the WT conduct an interactive replay of the test, where possible using live production systems, to review the impact of the actions of the RT provider.	✓	
The TCT, supervisors/overseers and TI provider are also present during these replay workshops.		✓
A purple teaming element is added in which the BT and the RT provider can 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.		✓
At the end of the test, there is a 360-degree feedback meeting which includes the entity, TI/RT providers and TCT. In this meeting, the parties review the TIBER-EU test process and give feedback.	✓	
After the BT and RT provider replay and 360-degree feedback workshop, the entity produces a Remediation Plan to address the findings. The Remediation Plan is agreed with the supervisor and/or overseer as part of their planning and control cycle.	✓	
The entity produces a Test Summary Report, which it shares with the lead authority.	✓	
The entity's board and the TI/RT providers sign an attestation to validate the true and fair conduct of the TIBER-EU test (to enable recognition by other relevant authorities).	✓	
If mutually agreed, the lead authority and/or the entity share the Test Summary Report and attestation with other relevant authorities (where applicable).	✓	
The TCT in each jurisdiction analyses the results of all the TIBER tests and the lessons learned from the 360-degree feedback meetings to produce high-level, aggregated findings. This information is used to enhance sector resilience and improve the TIBER-XX framework.	✓	

11.2 Responsibility Assignment Matrix for a TIBER-EU test

Table 5

RACI Matrix

Requirement	Responsible	Accountable	Consulted	Informed	Documents
Adoption and implementation					
The TIBER-EU framework is adopted and implemented	Authorities	Authorities	Financial and cyber security sector	Financial and cyber security sector	Notice to TIBER-EU Knowledge Centre and TIBER-XX Guide
Preparation phase					
Pre-launch meeting	TTM	TTM	WT	n/a	TIBER-XX Guide, TIBER-EU Services Procurement Guidelines, TIBER-EU White Team Guidance
Launch meeting	WT	Board of entity	TTM	n/a	n/a
Procurement process and formal contracts between the different stakeholders	WT	Board of entity	TTM	TI/RT providers	TIBER-EU Services Procurement Guidelines, contracts
Pre-test risk assessment	WT	Board of entity	TTM	TI/RT providers	Risk assessment

Requirement	Responsible	Accountable	Consulted	Informed	Documents
Scoping meeting	WT	Board of entity	TTM	TI/RT providers, if available	TIBER-EU Scope Specification document
Testing phase: threat intelligence					
Produce GTL Report for financial sector	Authorities and/or sector and/or TI providers	Authorities and/or sector and/or TI providers	Possibly national intelligence agency/ national cyber security centre/ high-tech crime unit	Authorities and/or sector	GTL Report
Produce a dedicated TTI Report on the entity, setting out threat scenarios which can be used by the RT provider	TI provider	WT	TTM, RT provider, possibly national intelligence agency/ national cyber security centre/ high-tech crime unit	n/a	TTI Report
Testing phase: red team test					
Handover session between TI and RT providers, providing the basis for the threat scenarios	TI provider	WT	RT provider, TTM	n/a	TTI Report
Scenario development for TIBER-EU red team test	RT provider	WT	WT, TTM, TI provider	n/a	Red Team Test Plan
Weekly test meetings or updates	WT	Board of the entity	RT provider, TTM	n/a	n/a
Discussion as flags are captured or when leg-ups are required	RT provider	WT	TTM	n/a	n/a
Closure phase					
Red Team Test Report, outlining the findings from the test	RT provider	WT	Senior executive responsible for cyber resilience at entity	TTM	Red Team Test Report
Blue Team Report, which maps the BT's actions alongside the RT provider's team actions	BT	WT	RT provider	TTM	Blue Team Report
Conduct an interactive replay of the test	WT	Board of entity	RT provider, TI provider, BT	TTM	n/a
360-degree feedback meeting	TTM	TTM	WT, BT, TI/RT providers	n/a	360-degree Feedback Report
Remediation Plan to address the findings	WT	Board of entity	TI/RT providers, TTM	Supervisor and/or overseer, if not involved during the test	Remediation Plan
Produce Test Summary Report	WT	Board of entity	TI/RT providers, TTM	Other relevant authorities	Test Summary Report
Signed attestation to validate the true and fair conduct of the TIBER-EU test	Board of entity	Board of entity	WT, TI/RT providers, TTM	TTM and other relevant authorities	Attestation

11.3 TIBER-EU documentation

This document, "TIBER-EU FRAMEWORK: How to implement the TIBER-EU framework", sets out the core foundational elements of the TIBER-EU framework for all EU authorities, entities, TI and RT providers, and all other relevant stakeholders.

This document should be used as a basis for each jurisdiction to determine how it will adopt the TIBER-EU framework for its own purpose.

For the implementation of the TIBER-EU framework, there are a number of accompanying documents which 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, authority and/or TI/RT providers to facilitate the overall test process.

These documents are listed below and can be requested from: TIBER-EU@ecb.europa.eu.

Table 6

TIBER-EU documentation

List of TIBER-EU framework documents	Responsible party
TIBER-EU FRAMEWORK: How to implement the TIBER-EU framework	Governing Council of the ECB
TIBER-EU Services Procurement Guidelines	Governing Council of the ECB
TIBER-EU White Team Guidance	Governing Council of the ECB
TIBER-XX Implementation Guide	(National) authorities
TIBER-EU Test Project Plan	Entity
TIBER-EU Scope Specification document (template available)	Entity
Generic Threat Landscape Report	(National) authorities or market
Targeted Threat Intelligence Report	Threat intelligence provider
Input for the Targeted Threat Intelligence (template available)	Entity
Red Team Test Plan	Red team provider
Red Team Test Report	Red team provider
Blue Team Report	Entity
360-degree Feedback Report	Entity
Test Summary Report (template available)	Entity and (National) authorities
Remediation Plan	Entity
TIBER-EU Attestation (template available)	Entity

Abbreviations

Term	Explanation
BT	Blue Team
CF	critical function
GTL	generic threat landscape
HUMINT	human intelligence
NDA	non-disclosure agreement
OSINT	open-source intelligence
RACI	Responsibility Assignment Matrix (RACI stands for Responsible, Accountable, Consulted, Informed)
RT provider	red team provider
TCT	TIBER Cyber Team
TIBER	threat intelligence-based ethical red teaming
TI provider	threat intelligence provider
TKC	TIBER-EU Knowledge Centre
TTI	targeted threat intelligence
TTM	Team Test Manager
TTP	tactics, techniques and procedures
WT	White Team
WTL	White Team Lead

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

For terminology and abbreviations, please refer to the ECB glossary.