TIBER-FI
Procedures and Guidelines

12 March 2025

Table of Contents

1 Introduction

Financial sector functions, services and data have long been in digital form, and it is crucial for the continued operation of this critical infrastructure to be able to protect these assets against cyber-attacks.

Financial sector entities make large investments in the cyber security design, implementation and monitoring of their information systems and services. In addition to these activities, it is also important to verify through testing that external attackers do not have opportunities to influence the operation and integrity of the services. The best way to achieve this is to apply testing methods that emulate how cyber criminals and other advanced threat actors assess the attack surface and execute their attacks.

TIBER-FI is a systematic, controlled and up-to-date cyber security threat intelligence-based framework and method for red team security testing. The objective of the framework is to produce findings for improving protection of the financial infrastructure and financial entities against targeted cyber-attacks.

The Bank of Finland owns and is responsible for the TIBER-FI framework in the Finnish financial sector. The framework implementation is based on TIBER-EU, maintained by the European Central Bank (ECB) and adjusted to accommodate local legal requirements in Finland and operational procedures set by Bank of Finland. To avoid unnecessary overlap between documents, TIBER-EU guidelines are referred to where possible in TIBER-FI procedures and guidelines.

The TIBER-FI framework is compatible with other national applications based on TIBER-EU. This allows cross-border cooperation in those cases where a financial entity is testing functions under several jurisdictions.

At the core of TIBER-FI are cyber security tests targeted at the critical information systems of the entities. Financial entities resource, plan and organise these tests themselves according to the procedure. The Bank of Finland supports the entities by providing guidance, a financial sector General Threat Landscape report (GTL), and test manager interaction throughout the testing process.

The objectives of the TIBER-FI framework are to

- support the cyber resilience of financial entities,
- improve the cyber resilience of the entire financial sector,
- advance good red team testing practices across the financial sector, and
- support cross-border testing of multinational entities.

Additionally, conducting a test project according to the TIBER-FI method will fulfil the requirements of DORA and DORA RTS for TLPT.

1.1 About the document

This document, dated 12 March 2025, contains the second major version of TIBER-FI. The first release was published on 29 April 2020 as a series of web pages on the www.suomenpankki.fi web site. Since then, the guidelines have had only minor updates, until this major release to accommodate the requirements and features of the Digital Operational Resilience Act (DORA), DORA Regulatory Technical Standards for Threat Led Penetration Testing (TLPT RTS), and the updated TIBER-EU.

This document is published at https://www.suomenpankki.fi/tiberfi by the Bank of Finland's TIBER-FI Cyber Team (TCT).

1.2 Contact

Enquiries about decisions regarding mandatory testing may be directed to the Finnish Financial Supervisory Authority (FIN-FSA).

Enquiries about TIBER-FI and this document may be directed to tiberfi@bof.fi.

Enquiries about an on-going test project may be directed to the assigned test manager or substitutes on that project.

1.3 Version history

12 March 2025	TIBER-FI 2.0 release based on requirements in DORA, TLPT RTS and TIBER-EU 2.0.

1.4 Abbreviations

Term	***Explanation***
BoF	Bank of Finland, Suomen Pankki
BT	Blue Team
BTTR	Blue Team Test Report
CIF	Critical or Important Function
CSP	Critical Service Provider
CT	Control Team
CTL	Control Team Lead
CTI	Cyber Threat Intelligence
DORA	Digital Operational Resilience Act
ESCB	European System of Central Banks
FIN-FSA	Finnish Financial Supervisory Authority, Finanssivalvonta
GTL	Generic Threat Landscape report provided by Bank of Finland
HUMINT	Human Intelligence

ICT	Information and Communication Technology
ISAC	Information Sharing and Analysis Centre
NDA	Non-Disclosure Agreement
OSINT	Open-Source Intelligence
PT	Purple Teaming
RACI	Responsibility Assignment Matrix
RTT	Red Team Testers
RTTP	Red Team Test Plan
RTTR	Red Team Test Report
TCT	TIBER-FI Cyber Team
TCT-FI	TIBER-FI Cyber Team, when needed to make the distinction
TIBER	Threat Intelligence-Based Ethical Red Teaming
TIBER-FI	TIBER implementation in Finland
TIP	Threat Intelligence Provider
TKC	TIBER-EU Knowledge Centre
TLPT	Threat Led Penetration Testing
TSR	Test Summary Report
TI	Threat Intelligence
TTIR	Targeted Threat Intelligence Report
TM	Test Manager
TTP	Tactics, Techniques and Procedures

Term	***TIBER-EU guidance in order of use***
CTG	TIBER-EU Control Team Guidance
IDG	TIBER-EU Initiation Documents Guidance
GSPP	TIBER-EU Guidance for Service Provider Procurement
GSSDG	TIBER-EU Scope Specification Document Guidance
TTIRG	TIBER-EU Targeted Threat Intelligence Report Guidance
RTTPG	TIBER-EU Red Team Test Plan Guidance
RTTRG	TIBER-EU Red Team Test Report Guidance
BTTRG	TIBER-EU Blue Team Test Report Guidance
PTG	TIBER-EU Purple Teaming Guidance
RPG	TIBER-EU Remediation Plan Guidance

TSRG	TIBER-EU Test Summary Report Guidance
AG	TIBER-EU Attestation Guidance

2 Stakeholders

This chapter introduces the stakeholders to TIBER-FI tests.

Annex 1 includes a detailed RACI matrix clarifying the roles and responsibilities within a TIBER-FI test.

2.1 TIBER-FI Cyber Team and test managers

The Bank of Finland has created the TIBER-FI framework and is responsible for providing guidance on its application. For this task, the central bank has appointed an internal **TIBER-FI Cyber Team** (**TCT-FI** or just **TCT** when the meaning is clear from the context).

The responsibilities of the TCT are to promote adoption of the TIBER-FI procedures, to coordinate the creation of the financial sector GTL report and to provide support and guidance for financial entities in the application of the procedures. The TCT is in contact with the European Central Bank's **TIBER-EU Knowledge Centre (TKC)** coordination group and the TCTs of other central banks.

A test manager (TM) is a person working on the Bank of Finland's mandate and is a member of the TCT. The role of the TM is to make sure that the entity undertakes the test in a uniform and controlled manner, and in accordance with the TIBER-FI framework and applicable requirements. Each test project will have a designated test manager with at least one alternate from the TCT.

2.2 The Control Team

For each TIBER-FI test, the entity must establish a **Control Team (CT)** with a dedicated **Control Team Lead (CTL)**. The Control Team holds key responsibilities pertaining to executing the test compliance with the requirements of TIBER-FI. The entity must base decisions about CT composition and appointing a suitable CTL on TIBER-EU Control Team Guidance (CTG). The CT must, to best of its abilities, work towards fulfilling all the requirements in the same guidance.

The CTL role is akin to a project manager. The CTL coordinates project management, test activities, information flow between the necessary stakeholders, and alignment with TIBER-FI requirements. The CTL may be an external consultant appointed by the entity.

The TM is independent from the CT and is not accountable for the CT's actions, the running of the test, and the outcomes, or the remediation planning. The CT must provide any information pertaining to the TIBER-FI test to the TM upon request.

2.3 The Blue Team

For each TIBER-FI test, the Blue Team (BT) comprises all staff at the entity, the entity's third-party service providers and any other party deemed relevant in consideration of the scope of the test, who are not part of the CT and are not

aware of the test. More 15 specifically, the BT is defending a financial entity's use of network and information systems by maintaining its security posture against simulated or real attacks. It is critical that the BT be completely excluded from the preparation and conduct of the TIBER-FI test. During the closure phase, when the BT is informed about the conduct of the test, the relevant and appropriate members of the BT should participate in the replay, Purple Teaming (PT) and remediation exercise, including the respective follow-up.

2.4 Threat Intelligence Provider, and Red Team Testers

A **Threat Intelligence Provider (TIP)** and **Red Team Testers (RTT)** are involved in each TIBER-FI test to deliver the core work. The main tasks of the TIP are to collect and provide threat intelligence and develop threat scenarios for red team testing. The RTT plan and execute attack scenarios on the target systems and services for purpose of validating cybersecurity controls and response, and identifying areas for their improvement.

As the testing takes place in live production environments, only an experienced TIP and RTT should be selected by the entity. It is essential that the TIP and RTT have the highest level of skills and expertise, strong ethical behaviour and an appropriate experience in threat intelligence and red team testing in the financial sector to be able to deliver effective and most qualified professional services and to reduce the risks. Both the TIP and the RTT must be knowledgeable about how to operate within the remits of the law in Finland with regard to processing information and conducting testing.

The TIP must follow the requirements in the TIBER-EU Targeted Threat Intelligence Report Guidance (TTIRG) for conducting the threat intelligence work.

Based on the DORA Regulation, it is mandatory to use an external TIP, and mostly external testers shall be used. The use of internal testers as RTT is possible according to DORA under specific conditions and upon TCT approval. The intention is that the internal testers should carry out TIBER tests as effectively and safely as external testers, without the security or the activities of the entity being endangered. When considering using internal testers as RTT, the entity should ensure that in every three tests they contract external testers as RTT and that RTT consisting of both internal and external testers are considered to be use of internal testers.

2.5 Affected personnel and service providers

During the TIBER-FI process, there are several activities that may be performed to mimic a real-life attack. Such activities require due consideration and evaluation in the context of existing laws and regulations. These activities may include

- gathering open-source intelligence (OSINT) data on the target entity, its suppliers, its employees and/or its customers,
- gathering data from other intelligence sources and the dark web related to the target entity, its suppliers, its employees and/or its customers,

- gathering account and password data from employees and service providers of the target entity.
- deployment of people into the entity under various guises to gather intelligence, and
- using targeting data gathered in the threat intelligence phase to create email, telephone, and in-person ruses as part of a scenario.

All TIBER-FI testing must be conducted in accordance with the relevant rules, laws and regulations (hereinafter together as “legislation”) applicable in Finland and other possibly affected jurisdictions. For this purpose, the entity, CT, TIP, and RTT must all be aware of the legislation in Finland concerning the topics of, inter alia, information security, personal data protection, insider information, criminal code, employment law, workplace privacy, anticompetition, outsourcing, immaterial rights, and other legislation related to information processing and activities during targeted threat intelligence and red team testing activities. The CT shall make sure during the procurement phase, and throughout the test project lifecycle, that all stakeholders are aware of the relevant legal boundaries, and only take legitimate actions.

The testing entity should consider well before engaging in TIBER-FI testing, whether there is a need for co-operation negotiations ("yhteistoimintaneuvottelut") about the methods of targeted threat intelligence and red team testing.

It is very likely that a TIBER-FI test will have an impact on the services procured by the testing entity, and therefore on the provider(s) of those services, whether they be, inter alia, ICT, staffing and/or security services. The testing entity should consider well before engaging in TIBER-FI testing, whether there is a need for changes to contractual agreements with service providers or for the setting up of mechanisms for notifications to such service providers.

All the actions mentioned herein must be carried out in full compliance with any and all secrecy obligations pertaining to any contemplated or on-going testing activities, and by ensuring that the test outcomes are uncorrupted by any disclosure.

2.6 Cross-border cooperation

The harmonised approach in TIBER-EU enables cross-border TIBER testing for multinational entities while ensuring focus on regional differences. It is the responsibility of the TCT to liaise with other authorities that potentially are relevant for the test of such a multinational entity.

In the beginning of the test, the entity will provide an overview of the entity’s operations in other Member States, which will be included in the assessment of whether a cross-border test should be conducted. Also, group structure and the setup of ICT systems in the group will be included in the assessment. Based on the result of the assessment, the TCT will reach out to the authorities in these Member States with the aim of establishing cross-border collaboration for the

test, including specifying the roles of all parties, or providing documentation for cross-border recognition of the test results.

3 Risk management of TIBER-FI tests

The TIBER-FI 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.

Throughout the conduct of the TIBER-FI test, the entity should ensure that it gives due consideration to the risks associated with the testing of live production systems of CIFs, including potential impacts on the financial sector and on financial stability at European and national level.

3.1 Risk assessment

The entity is accountable for managing the risks pertaining to TIBER-FI testing. The CT should therefore remain in control of the testing process and continuously identify, analyse, evaluate and treat the relevant risks in an effective manner.

The CT should conduct a risk assessment before and during the test. The risk assessment should be well documented, reviewed and updated when needed, such as when the attack scenarios have been developed. Before the testing phase commences, the CT should consult the TM on the risk assessment. Risks to be considered relate to at minimum

- the procurement of providers,
- the level of confidential data to which these providers gain access,
- crisis and incident escalation,
- the interruption of critical activities and/or impact of provider activities on the entity and its third parties, and
- the incomplete restoration of systems affected by the test.

In addition, risks that are common to red team testing projects must be considered, such as uncontrolled disclosure of the project, delays due to unavailability of key resources, and difficulty in producing effective leg-ups in timely manner.

When several entities are involved in a multi-party test, the CT of each entity shall conduct its own risk assessment, also taking into consideration the services offered by ICT third party service providers. The CT of the entity assigned to direct the test shall also conduct a risk assessment for the aspects of the test specific to the involvement of several entities. Moreover, the CT of the involved entities should work together to identify potential joint risks, including those related to the use of a common ICT third party service provider and the offered services (e.g. regarding a single point of failure).

3.2 Minimum requirements for providers

A key means of managing the risks associated with the TIBER-FI test is to use the most competent, qualified and skilled TIP and RTT with the required experience to conduct such tests. Consequently, prior to the engagement, the entity must ensure that the TIP and RTT are free from conflict of interest and meet the minimum requirements evidenced by the relevant documentation and certifications. The minimum requirements are set out in the TIBER-EU Guidance for Service Provider Procurement (GSPP).

Where feasible, entities should ensure that the providers are accredited and certified by a recognised body as being able to conduct a TIBER-FI test. There is currently no accreditation system for TIBER-FI service providers in Finland.

3.3 Contracts

The contracts with the TIP and RTT shall include

- a requirement for the providers to meet security and confidentiality controls or standards defined by the underlying entity,
- a formal code of conduct or an ethical framework that the providers adhere to,
- the protection of parties involved (e.g. indemnifications),
- a clause related to data destruction requirements after the test,
- a clause related to breach notification, and
- activities that are not allowed during the test, such as: unauthorised destruction of equipment, uncontrolled modification of information and ICT assets, intentional compromise of the continuity of CIFs of the tested entity, unauthorised inclusion of out-of-scope systems, unauthorised disclosure of test results, blackmail, threatening or bribing employees.

In case of a multi-party test, the same external RTT and TIP shall be used for the purpose of conducting the test. The testing entity and the other participating entities should have a mutual agreement on the aspects above with the selected TIP and RTT. The GSPP sets out in greater detail agreement checklists for the entity and TIP/RTT to consider when formalising their contractual agreements.

4 Generic threat landscape

A Generic Threat Landscape (GTL) report is provided by the TCT for all TIBER-FI tests. This report is sourced from a highly competent provider of cyber threat intelligence to offer a reusable cost-effective tool for test projects to make use of.

The GTL report elaborates on the specific threat landscape in Finland and the Nordics. The report is to be used during the preparation phase of TIBER-FI, and it complements the production of the work during the TTI process step.

The GTL report is updated at least annually, and a testing entity may complement it with other high quality intelligence sources during a test project.

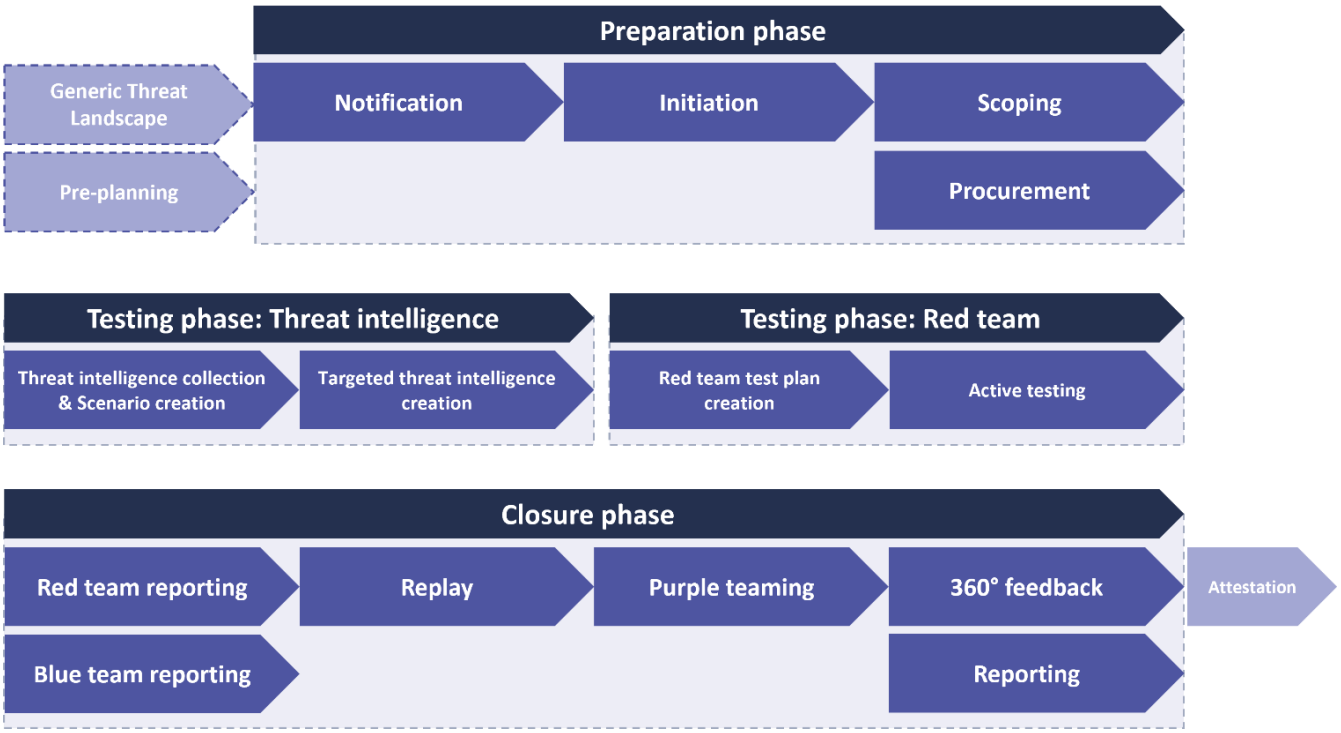
5 TIBER-FI process

This chapter gives an overview of the TIBER-FI timelines and durations for phases, deliverables, and meetings. The DORA Regulation and DORA RTS for TLPT set out requirements regarding activities, their timelines and deliverables, and these requirements are incorporated into the TIBER-FI procedures and guidelines.

The phases to a TIBER-FI test are:

1. Pre-planning (informal)
2. Preparation phase
3. Testing phase: Threat intelligence
4. Testing phase: Red team testing
5. Closure phase

Each formal phase is divided into process steps and activities.



5.1 Pre-planning

The pre-planning phase consists of preparatory dialogue between the TCT and the designated points of contact at the entity.

The objective of pre-planning is to ensure that the entity is familiar with the TIBER-FI process and are informed of expectations about resource allocations, project deliverables, practical arrangements of a test project, and other such topics. Potential cross-border aspects of the test project should be explored at this point.

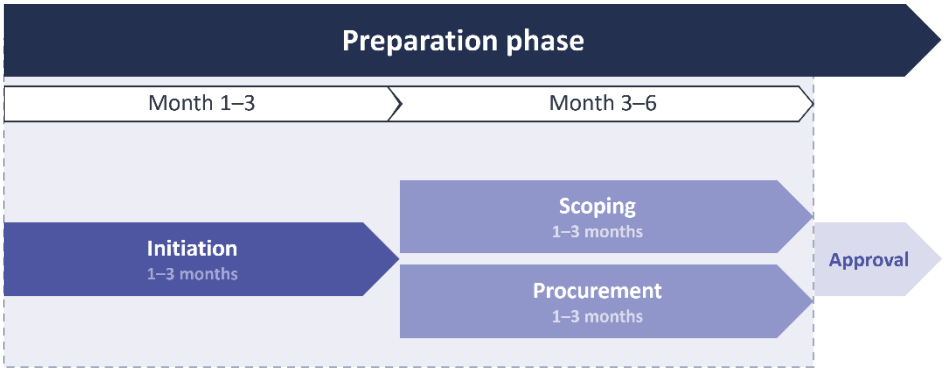
Engaging in this activity does not indicate a formal start of the testing process.

5.2 Preparation phase

The preparation phase is the formal start of a TIBER-FI testing project. The phase is composed of four process steps:

1. Notification
2. Initiation
3. Scoping
4. Procurement.

The process steps and activities in the preparation phase should be finished within a **maximum of six months**.



Activities and deliverables of each process step is discussed in the following chapters.

5.2.1 Notification

A TIBER-FI test project and its preparation phase **formally begins** when the designated points of contact from a financial entity receive a notification letter from the TCT, and the TM starts liaising with the entity. The activities of the entity in the preparation phase should be finished within a maximum of six months after the receipt of the written notification.

The notification letter includes target dates set by the TCT for key TIBER-FI phases, process steps, activities, or deliverables. These dates and the overall timeline shall be aligned with the entity at a notification meeting.

Shortly after the notification letter, the TM holds a notification meeting with the entity. During the notification meeting, the TM will brief the entity on

- its designation to carry out a mandatory or voluntary test,
- the TIBER-FI testing process, its elements and deliverables,
- the stakeholder roles and responsibilities, and
- the TCT and CT composition.

Together with the TM, the entity shall identify additional entities or legal parties which may have to be involved in the test.

Required deliverables and meetings

Title	*Responsible party*
Notification letter	TCT
Notification meeting	TCT

Required activities

1. TCT shall deliver the notification letter.
2. TCT shall conduct a notification meeting with the entity.

References

- TIBER-EU Control Team Guidance
- TIBER-EU Initiation Documents Guidance

5.2.2 Initiation

The next process step in the preparation phase is the initiation of the project. During this process step, the entity prepares **the initiation documents**, which include a project charter – comprising a high-level project plan – and communication details and channels to be established. Moreover, the code name for the TIBER test is determined. The information regarding any planned or ongoing test is limited on a need-to-know basis, including the management body of the entity. However, the CT must ensure that the management body of the entity is informed about the progress of the test and its associated risks.

As the CTL is responsible for all test preparations and test activities, including coordination with the TIP and RTT and meetings with the TCT, it is very important that the CTL is appointed as early as possible. It is foreseen that the CTL will use a substantial amount of time during all phases of the TIBER-FI test and they are expected to be a senior resource with excellent project management and communication skills. The CTL plays a key role in the safe conduct of a TIBER-FI test and should therefore have a sufficient mandate within the entity to guide all aspects of the test whilst safeguarding its confidentiality. In appointing a CTL, both role, in-depth knowledge of the entity, strategic positioning, seniority and access to the management board should be considered.

As part of the initiation documents, the CT should arrange the entity's own organisation of the management of the TIBER-FI test. The entity must follow the requirements in the TIBER-EU Control Team Guidance (CTG) in establishing a CT.

The CTL will inform the TCT of the members included in the CT by adding the relevant names and contact information to the initiation documents. The TCT must validate the initial composition of the CT along with any subsequent composition changes.

The CT should ensure that access to information pertaining to any planned or ongoing TIBER-FI test is limited on a need-to-know basis to the CT, the entity's management body, the TCT, TI and RTT. To safeguard secrecy, staff members of the entity outside of the CT must only be made aware of a planned or ongoing TIBER-FI test for cogent reasons and by prior agreement with the TCT. This ensures secrecy is upheld as effectively as possible, even in cases of test activities being detected. As an added measure, the entity may at their discretion require CT members to sign a non-disclosure agreement (NDA) to ensure the internal/external confidentiality of the test.

Furthermore, it should be anchored whether the entity will use an external provider as RTT, internal testers as RTT, or both. At this point in time, if the entity intends to use internal testers as RTT, it is expected that the entity will have already submitted the formal application required to the TCT, and that the TCT will have made the assessment and informed the entity thereof.

Since testing is conducted on live production systems, the CT should establish comprehensive risk management measures during the preparation phase to address all potential risks arising from the conduct of the test.

The initiation documents must include the required content as outlined in the TIBER-EU Initiation Documents Guidance (IDG).

The CT must send the initiation documents to the TM **no later than 3 months** after the written notification.

Required deliverables and meetings

Title	***Responsible party***
Initiation documents	Entity
Initiation meeting	TCT

Required activities

1. The entity shall prepare and submit all initiation documents to the TM.
2. The TM shall validate all initiation documents, including the core testing components, and formally notify the CT of successful validation.

References

- TIBER-EU Control Team Guidance
- TIBER-EU Initiation Documents Guidance

5.2.3 Scoping

During the scoping process step, the tested entity must complete a TIBER-EU Scope Specification document (SSD) listing the CIFs, the systems and services underpinning each CIF, as well as the flags to be captured for each system.

Entities may conduct a business impact analysis defining the CIFs as part of their standard business continuity management or operational risk management practices, which may be used as input. CIFs need to be identified on a comparatively high level and might be aggregated to more abstract CIFs. For large and complex entities with numerous CIFs, it may not be feasible to conduct an effective test with all CIFs in the scope of a single test. In this case, there needs to be a rationale on why certain CIFs are not included in the test, which is clearly outlined within the SSD.

Entities across the sector support and deliver these CIFs 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 operating them that are the focus of TIBER-FI tests. In most cases, this will also include the systems, people and business processes underpinning the entity's CIFs that are outsourced to third-party service providers. The entity may decide at its discretion to include additional non-critical components in the scope, provided the inclusion does not negatively affect the testing of the CIFs, e.g. pre-production, testing, backup and recovery system.

Required deliverables and meetings

Title	***Responsible party***
Scope specification document	CT
Scope meeting	TCT

Required activities

1. The CT shall develop and document the complete scope specification and submit the document to the TM.
2. The TM shall validate and approve the scope specification and formally notify the CT of the approval.

References

- TIBER-EU Guidance for Service Provider Procurement
- TIBER-EU Scope Specification Document Guidance

5.2.4 Procurement

It is critical for safe and secure execution of TIBER-FI testing that the TIP and RTT possess the highest levels of skills, capabilities and qualifications. The entity must therefore select the TIP and RTT with the requisite skills and experience to perform the test.

To ensure that the TIP/RTT meet the appropriate standards for conducting such a test, the entity should conduct its own due diligence as part of its procurement process and existing risk management practices to ensure that the procured TIP and RTT meet the minimum requirements set out in the GSPP.

Responsibility for ensuring that the appropriate TIP/RTT are selected lies solely with the entity. The CT should document its assessment of compliance and provide evidence of compliance to the TM. The CT shall not proceed with contracting the selected TIP/RTT in the event that the TM assesses that the selected providers do not ensure compliance.

In exceptional circumstances, the entity could end up having to contract testers that do not meet the minimum requirements for providers. In such a case, the entity is required to adopt appropriate measures mitigating the risks related to the lack of compliance with the requirements and provide evidence of these measures to the TM.

The procurement of providers must be finalised before the start of the testing phase. The entity should start the procurement process as early as possible to ensure that there are no bottlenecks or delays in the overall testing process.

After the contracts with the TIP and the RTT have been signed, the CT organises a launch meeting where actions include

- onboarding TIP/RTT,
- presenting the CT composition and project plan,
- presenting the scope, as available,
- presenting the test process and the rules of engagement,
- presenting the communication details and channels, and
- discussion between the stakeholders about their expectations and cooperation.

Required deliverables and meetings

Title	***Responsible party***
Launch meeting	CT

Required activities

1. The CT shall complete procurement of the TIP and RTT and formally onboard them to the testing program.
2. The CT shall arrange an official launch meeting with at least the CT, TM, TIP and RTT participating.

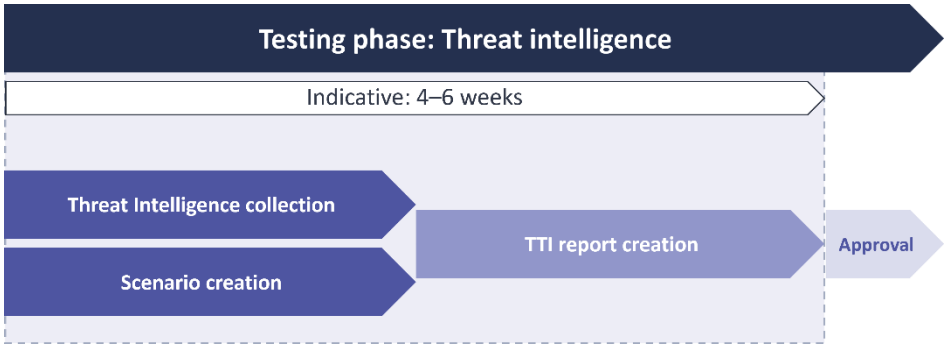
References

- TIBER-EU Guidance for Service Provider Procurement

5.3 Testing phase: Threat intelligence

Once all activities in the preparation phase are concluded, the testing phase officially starts with the threat intelligence (TI) component. The threat intelligence phase consists of two process steps, namely i) TI collection and scenario creation and ii) creation of the Targeted Threat Intelligence Report (TTIR). Threat intelligence-based scenarios mimicking real-life cyber adversaries are essential to the realism and success of testing activities. During TI collection and scenario creation, the TIP collects, analyses, and disseminates tailored intelligence related to two key areas of interest

- **target intelligence**: information on potential attack surfaces and exposures across the entity, and
- **threat intelligence**: information on relevant threat actors and probable threat scenarios.



Activities and deliverables of each process step is discussed in the following chapters.

5.3.1 Threat intelligence collection

For the TIBER-FI framework to work effectively, it is critical that the TTI 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 threat actors themselves, including their intent, capability and modus operandi.

The TIP is expected to

- engage with the entity to obtain useful context for conducting the threat analysis,
- be able to adequately cooperate with the internal threat intelligence capabilities (Cyber Threat Intelligence; CTI) of the testing entity,
- use a broad range of sources, e.g. internet services, a mixture of public and private forums and a range of media types such as internet relay chats, email and video,
- have a depth of sources,
- only use TI gathering techniques that do not risk compromising the secrecy of the test,
- have adequate language support,
- be able to use a variety of methods in intelligence gathering, for example OSINT and HUMINT,
- demonstrate strong ethical behaviour, and
- cooperate with the RTT in a flexible and transparent manner, when required, in the testing process.

The TIBER-FI process is designed to create realistic threat scenarios describing attacks against an entity. These scenarios can be used by the RTT to guide their intelligence-led 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 CIFs that form the scope and target of the test.

While this approach is highly valuable, real-world threat actors may have months to prepare an attack. In addition, while TIPs are constrained by limitations on the time and resources available, and by moral, ethical and legal boundaries, real-world threat actors are free of such constraints. This difference can cause difficulties when attempting to design realistic scenarios that can be executed within those boundaries, as sensitive data about the target, e.g. knowledge about the internal network, is often hard to gain using morally, ethically or legally justifiable techniques.

Similar constraints apply to CIFs, which are internal to the entity and typically do not have a large footprint in the public domain. They also apply to the systems that underpin CIFs, 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 TIP should seek from the entity and be provided with

- a business and technical overview of each CIF-supporting system in scope,
- the current threat assessment and/or threat register,

- examples of recent attacks on the entity or its environment, and
- previous TTIRs used in TIBER tests, if relevant and deemed feasible by the entity.

The entity should provide the above information to the TIP to facilitate scenario development. In cases where the entity has an internal CTI function, the TIP could liaise with it and gather relevant information that will help inform the TTIR. Prior to liaising with the internal CTI capability of the testing entity with the TIP, the CTL should take appropriate measures to safeguard the confidentiality of the test. Finally, in cases where the respective jurisdiction(s) has/have produced a GTL report, the TIP should use this as a basis for producing the TTIR, focusing on how to contextualise the threat landscape of the country, the different threat actors and the common vulnerabilities to the specificities of the entity.

To identify targets, the TIP 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 TI to be put into context and will contribute to the development of the threat scenarios in the TTIR. Part of this information should be provided by the entity using the TIBER-EU Targeted Threat Intelligence Report Guidance (TTIRG). The output of this activity is the identification, on a CIF-focused, system-by-system basis, of the attack surfaces of people, processes and technologies related 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. The TTI gathering 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 RTT's deeper and more focused targeting activities.

Required deliverables and meetings

Title	***Responsible party***
Status updates	TIP

Required activities

1. The TIP shall conduct threat intelligence activities.

References

- TIBER-EU Targeted Threat Intelligence Report Guidance

5.3.2 Scenario creation

In this process step, a broad set of scenarios called a **scenario longlist** is created by the TIP and presented to the stakeholders during a **scenario selection meeting**. The scenarios must be based on intelligence acquired during the target identification process and should present a credible picture of the entity's cyber threat landscape, i.e. threat intelligence-based and specifically tailored to the entity's business environment, including its key threats and detailed profiles of the threats and actors with the highest scores. Based on the scenario longlist, the final scenarios used for testing will be selected.

While the threat scenarios are fictional, they should be based on real-life examples of cyberattacks including the motivations of the attackers, their objectives, and the methods they employ to meet them. By focusing on what is realistic rather than theoretically possible, the scenario identification supports the RTT in justifying the approach they plan to take.

In addition to threat-led scenarios, the TIP may develop other types of scenarios. For example, in cases where the use of conventional or intelligence-backed TTPs may not be successful in achieving a flag. To emulate a real-life attacker in such a case, the TIP could deploy creative and innovative TTPs. Along these lines, the TIP 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. Such scenarios may include hybrid, novel TTPs and "out of the box" elements. Also, a certain scenario might be of great relevance to a tested entity, even though it is not threat-led.

A maximum of one scenario (out of the three selected scenarios) per TIBER-FI test may be non-threat-led, allowing for the investigation of future or otherwise relevant attack vectors. Such a scenario is referred to as a **scenario X**. If no scenario X is specified during the threat intelligence phase, a maximum of one scenario may be transformed into a scenario X during the active testing phase, after agreement of the TM, CT and RTT. For example, a scenario X could be developed based on the entity's unique technology stack or ICT architecture that presents potentially exploitable paths without corresponding threat intelligence precedents. This approach allows testing of entity-specific vulnerabilities that sophisticated attackers might identify but have not yet been observed in the wild.

In case of a multi-party test involving an ICT third party provider, at least one of the selected scenarios should cover the ICT third party providers' systems, processes and technologies supporting the CIFs of the entities in scope.

Based on the information of the collected TI and the selected scenarios, the CT must start to plan for the potential use of **leg-ups**. Leg-ups are network and system accesses and/or devices that may be needed by the RTT in their execution of the scenarios. Leg-ups could also include additional information on target systems and technology. The RTT are invited to offer their expert view on what kind of leg-ups would be more suitable. It should be noted that actions such as directly providing access to the flags and/or disabling security controls should not be proposed as leg-ups.

During the **scenario selection meeting**, the TIP introduces a broad set of realistic attack scenarios, based on the collected entity-tailored TI and an evaluation of every CIF in scope of the test. The scenario selection meeting is held when the longlist with scenarios is ready to be shared and discussed. The participants in this meeting are the CT, TM, TIP, and RTT.

The CTL selects/adapts three or more scenarios to be followed during testing, based on

- the recommendation of the TIP, considering the threat-led nature of the scenarios,
- the input provided by the TM,
- the feasibility of the proposed scenarios for execution, based on the expert judgement of the RTT,
- strategic criteria (e.g. regarding scenarios of past tests, the need for leg-ups), and
- the size, complexity and overall risk profile of the entity and the nature, scale and complexity of its services, activities and operations.

Required deliverables and meetings

Title	***Responsible party***
Scenario longlist	TIP
Scenario selection meeting	CT
Scenarios selected for testing	CTL

Required activities

1. The TIP shall prepare the longlist of realistic attack scenarios.
2. The CT shall arrange a scenario selection meeting with at least the CT, TM, TIP and RTT participating.
3. The CTL shall decide on which scenarios to proceed with.

References

- TIBER-EU Targeted Threat Intelligence Report Guidance

5.3.3 TTI report creation

This process step focuses on the finalisation of the TTIR, which is a bespoke, report for the entity being tested. The TTIR creation process step builds on the initial TI work completed during the TI collection and scenario-creation process step. Responsibility for the development and production of the TTIR lies with the TIP. After the scenario selection meeting, the RTT are more involved, absorbing the contents of the TTIR and preparing to integrate the attack scenarios into a

RTTP. To enrich the TTIR, the RTT are encouraged to give feedback during the final stage of the TTI process. Two elements are particularly relevant to provide a firm TI basis for the RTTP:

- tailored scenarios, which will support the formulation of a realistic and effective RTTP,
- threat actor goals, motivations and TTPS, which will help steer the RTT in its attempt to capture the flags.

In addition, based on the TTI report, the CT and TM may opt to update or modify the flags. The CT should update their risk management controls after the receipt of the TTI report, where applicable. After finalisation, the CT should send the TTI report to the TM for approval, who will notify the CTL accordingly.

During the **TTIR meeting**, the TIP should present

- the collected target intelligence,
- the selected and elaborated scenarios for testing – in detail
- the draft TTIR.

All stakeholders should provide feedback on and discuss the report, identifying potential aspects to be added/changed. If necessary, flags might be updated in the light of the report data, and potential leg-ups should be explained. The TTIR meeting is held as soon as the report is in its final stage.

The participants in this meeting are, at least the CT, TM, TIP and RTT.

The TIP delivers a dedicated **TTI report**, containing the required elements as described in the TTIRG, outlining the entity tailored threat landscape as well as describing the selected scenarios in detail.

Required deliverables and meetings

Title	***Responsible party***
TTIR draft	TIP
TTIR meeting	CT
TTIR final	TIP

Required activities

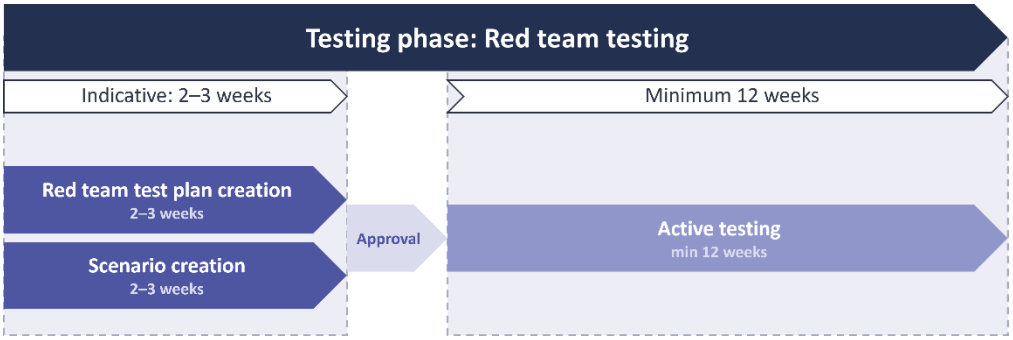
1. The TIP shall prepare a draft TTIR.
2. The CT shall arrange a TTIR meeting with at least the CT, TM, TIP and RTT participating.
3. The TIP shall provide the final TTIR.
4. The CT shall send the TTIR to the TM for approval.
5. The TM shall notify the CTL of TTIR approval.

References

- TIBER-EU Targeted Threat Intelligence Report Guidance

5.4 Testing phase: Red team testing

Following the approval of the TTIR by the TM, the RT activities move into focus. During the red-teaming phase, the RTT plan and execute a TIBER test based on the respective selected scenarios for the target systems and services that underpin the selected CIFs in scope.



The red-teaming phase consists of two separate process steps, namely (1) the Red Team Test Plan (RTTP) creation and (2) the active testing. The TTIR forms the basis of the RTTP. When the RTTP is in its final stage, the stakeholders hold a RTTP meeting, after which the plan is approved. After approval of the test plan by the CT and the TM, the active testing process step starts. During the active testing, the RTT aim to reach all the flags, as defined in the test plan.

The RTT should deploy a range of TTPs during the test. The following list is just one example of a testing methodology that the RTT 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 critical steps and can lead to significant discovery about the target's people, processes, technology, surroundings, and environment. This step may also involve building or acquiring specific tools for the engagement.

Weaponisation – By thoroughly analysing information gathered about the infrastructure, facilities and employees, the RTT begin to form a picture of the target and its primary operations. Effective weaponisation involves preparation for the operations specific to the targets.

Delivery – This marks the active launch of the full operation. The RTT begin to carry out the actions 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 RTT's goal is to "break in", i.e. to compromise servers/apps/networks, and to 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 achieved, 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 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 RTT aim to complete the test and achieve the objectives and capture the flags.

The TIBER-FI 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 TIP/RTT 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 CIFs, 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 RTT 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 RTT on the scenarios chosen, including on the people, processes and systems targeted in the scenario. This information may give the RTT 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-FI 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 TIP/RTT, the more the participating entity will gain from the test. It should be evident, however, that the information given to the TIP could have been obtained by an advanced attacker with more time and unhindered by moral, ethical and legal constraints.

During the testing phase, the RTT may be unable to progress to the next stage owing to time constraints or because the entity has been successful in protecting itself. In such scenarios, the RTT, with approval from the CT and TM, may be given a leg-up, for example where the entity essentially gives the RTT access to its system, internal network, etc. to continue with the test and focus on the next flag/target. The leg-ups are usually, but not limited to, system or network access, information on targets, etc. 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. It is important that the CT, in consultation with the TM, stands ready to provide a leg-up and does not unduly delay the test.

In addition to the information provided by the entity, the role of the TIP can be enhanced during the testing phase. For the test to succeed, the TIP can provide ongoing TI to the RTT 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 TI while attempting to compromise an entity. Allowing a fluid relationship between the TIP and RTT during the test may add greater value to the test. Where the TIP and RTT decide to work more closely during the test, the working arrangements and information sharing arrangements must be agreed between the two parties.

5.4.1 Red team test plan creation

In this process step, the RTT develops and integrates the attack scenarios into a RTTP, leveraging on the scenarios included in the TTIR.

The RTT should align their test objectives with the goals of each of the actors, map these to the CIF-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 RTT should therefore adapt their attack methodology to replicate the real-life attack scenarios.

The RTT 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 RTT should therefore include an appropriate plan to assist the entity in managing these risks.

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 RTT 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. 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.

Scenarios to be tested may also include the usage of TTPs which look to breach the physical security of the entity to gain access to the network or plant a device. If such a method is used, however, appropriate safeguards (e.g. formal consent by the entity) should be in place and no legal boundaries should be crossed. The risk of detection from each scenario must also be taken into consideration when drafting the test's timeline and setting up the order of scenario execution.

The output of this activity is the final RTTP, 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, including the frequency of test progress reports with the CT and the TM.

The RTTP shall include the required content as defined in the TIBER-EU Red Team Test Plan Guidance (RTTPG).

Once the RTTP is in its final phase, the RTT, TM, CT, and the TIP, where appropriate, come together to discuss it during the RTTP meeting. The RTT explain their envisioned approach to reach the flags, as well as the technical measures they will take for doing so, and the leg-ups they might require at certain points. During the RTTP meeting, the RTT shall present

- the planned attack steps for each end-to-end scenario, including detailed flags and expected leg-ups,
- time planning for each scenario,
- dedicated milestones and leg-ups,
- escalation contacts and procedures,
- rules of engagement and reporting agreements, and
- risk management measures taken by the RTT.

All stakeholders should provide feedback on and discuss the test plan, identifying potential aspects to be amended.

The participants to this meeting are at least CT, TM, RTT and TIP (where appropriate).

The CT and the TM approve the final RTTP – and any subsequent changes to it – which should include, if any, the feedback received during the meeting.

Upon finalisation of the RTTP, the CT must update its risk management controls and prepare specific leg-ups for the RTT, by being ready to execute all necessary processes and procedures without raising alarm and causing delay.

Required deliverables and meetings

Title	***Responsible party***
RT test plan	RT
RT test plan meeting	CT
Updated risk management plan	CT

Required activities

1. The RT shall prepare a draft RTTP.

2. The CT shall arrange a RTTP meeting with at least the CT, TM and RTT participating.
3. The CT shall send the RTTP to the TM for approval.
4. The TM shall notify the CTL of RTTP approval.
5. The CT shall update its risk assessment and amend controls as needed.
6. The CT shall make note of the proposed leg-ups and, where relevant, start preparations about them.

References

- TIBER-EU Red Team Test Plan Guidance

5.4.2 Active testing

Once the RTTP is approved by the CT and TM, the RTT should initiate the active execution of the test. Any changes to the RTTP after its approval must be approved by the CT and TM. The attack scenarios are not a prescriptive playbook which must be followed precisely during the test. If obstacles occur, the RTT should show their creativity (as advanced attackers would) to develop alternative ways to reach the test objective or flag.

A minimum of 12 weeks must be allocated to active testing. This allows the RTT to conduct a realistic and comprehensive test in which all attack phases are executed and the flags can be reached. Within this time frame, attack scenarios can be executed in parallel or in sequence. When executing scenarios in parallel, the RTT still needs to complete all the scenarios' in-through-out phases.

The RTT are constrained by the time and resources available as well as by moral, ethical and legal boundaries. It is therefore possible that the RTT may require occasional leg-ups in addition to those laid out in the test plan to help the RTT progress. All leg-ups are to be provided by the CT, and approved by both the CT and the TM.

During the execution of the test, it may happen that a staff member of the entity or its ICT third-party service provider irrevocably detects the RTT via its activities. In such cases, the CT should propose and submit measures allowing the continuation the test to the TM for its validation while ensuring that the secrecy of the test is upheld. Other cases may include the discovery of an actual compromise or any other exceptional circumstances triggering risks of impact on data, damage to assets, disruption to CIFs, services or operations. Under such exceptional circumstances, after consultation with the TM, the CTL may suspend the test as needed to thereby facilitate delays or employ other changes to continue the test and maximise its learning experience.

In the event that a critical vulnerability is discovered during this phase, the CT may also initiate remediation actions, based on technical feedback provided by the RTT, and in close consultation with the TM, while ensuring the minimum possible impact onto the testing activities and confidentiality.

As a last resort, if continuation of the test is not otherwise possible, and insofar as is possible strictly within a scenario, testing activities can be continued as a limited PT exercise during the testing phase – subject to prior validation by the TM. The duration of the limited PT exercise counts towards the 12-week minimum duration of the active red team testing phase.

Irrespective of the methodology used by the RTT, the test should be conducted in a controlled manner, taking a stage-by-stage approach, and in a way that minimises risks to the entity and its CIFs. All of the RTT actions should be logged: for the replay exercise with the BT, as evidence for the RTTR, and for future reference.

The CT, TIP, RTT and TM should agree on the concrete end of the active RT phase.

Following the end of the active RT phase, the CTL will inform the BT that a test was conducted. After the test, the RTT and TIP should carry out restoration procedures, to safeguard the integrity of the tested entity's environment. These restoration procedures should be planned and coordinated with the CT and BT, and ideally should not occur before the replay and PT exercise in the closure phase. The procedures include the deletion of information related to passwords, credentials (or changing them) and other (secret) keys compromised during the test. It also entails the restoration and deletion of compromised secure communication channels to the entity, secure collection, storage, management and disposal of collected data. Technical restoration procedures should include

- command and control deactivation,
- scope and date kill switches,
- removal of backdoors and other malware,
- potential breach notification,
- procedures for future back-up restauration which may contain malware or tools installed during the test, and
- monitoring of BT activities and information to the CT of any possible detections.

Required deliverables and meetings

Title	***Responsible party***
Daily and weekly updates	RT
Flags, milestones, and leg-ups	CT
Restoration activities	CT

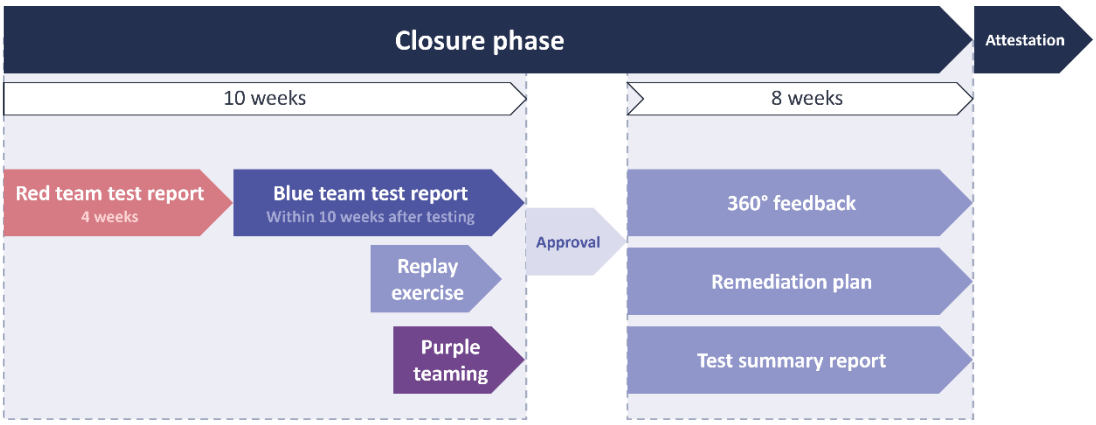
Required activities

1. The RTT shall complete the planned and required testing.

2. The CTL shall inform the BT that a test was conducted.
3. The CT shall coordinate the planning of restoration activities.
4. The RTT and TIP shall carry out restoration activities, where appropriate.

5.5 Closure phase

The closure phase allows all relevant stakeholders to reflect on the outcome of the test and make improvements to further enhance the cyber resilience of the entity.



Once the active testing is concluded and the BT has been informed about the test, the RTT and the BT start to prepare their respective test reports. The RTTP includes details of the approach taken to the testing and the findings and observations from the test, whereas the BT Test Report (BTTR) includes details on the observations of the BT during the test, mapped alongside the actions of the RTT.

Once these reports are in their final stage, the replay process step commences, followed by the PT process step. After the replay and PT process steps, the CT finalises the test summary report and remediation plan. When the PT step has concluded, the 360° feedback process step commences, during which all relevant stakeholders deliver feedback on each other, and the overall testing process. The test is concluded with remediation planning and result sharing.

The first part of the closure phase, containing the writing of the RTTR and BTTR and the replay and PT exercises, takes a maximum of 10 weeks. The second part of the closure phase relates to the TM's assessment of the BTTR and the RTTR. The third part of the closure phase, related to the 360° feedback and the writing of the test summary report and the remediation plan, takes a maximum of 8 weeks. Finally, the closure phase ends with the test attestation. Depending on the time the TM needs for the assessment of the RTTR and BTTR, the total duration of the phase may be longer than 18 weeks.

5.5.1 RT and BT reporting

These process steps commence after the active testing has been concluded and the key members of the entity's BT are informed about the test. The RTT produces a RTTR, for delivery to the CT within four weeks after the end of the active red team testing phase, which in turn delivers it to the BT and the TM. It is then used by the BT to deliver the BTTR, no later than 10 weeks after the end of the active red team testing phase, to the CT, which in turn delivers the BTTR to the RTT and TM. The BTTR should be drafted ahead of the replay and PT exercises. In the BTTR, the BT maps its actions alongside the RTT's actions. Both reports are expected to contain a timeline of events and detections that occurred during the exercise together with any other relevant information.

It is important to note that the RTTR and BTTR are highly sensitive. As such, access to these reports, their dissemination, retention and destruction must be controlled. At the request of the TM, the reports might be redacted of sensitive information. The CT shall control the distribution of the reports between the stakeholders.

The TM assesses whether the RTTR and BTTR contain the required information and provides feedback where necessary. Given the importance of the RTTR for the BTTR and the replay exercise, it is advised that the TM provide feedback on the document during final stage.

Required deliverables and meetings

Title	***Responsible party***
Red Team test report	RT
Blue Team test report	BT

Required activities

1. The RT shall deliver the RTTR within 4 weeks after the end of active testing.
2. The BT shall deliver the BTTR within 10 weeks after the end of active testing.
3. The CT delivers the reports to the BT, RT, and TM.
4. The TM shall assess the reports and notify the CT of the feedback on the report and the completion of assessment.

References

- TIBER-EU Red Team Test Report Guidance
- TIBER-EU Blue Team Test Report Guidance

5.5.2 Replay exercise

After the RTT and BT deliver their reports, the CT arranges a replay exercise. The participants in this exercise are, at least the CT, BT, RTT, and TM (if feasible) and it usually takes the form of one or more workshops.

Although the exercise should be held within 10 weeks after the end of the active red team testing, it is highly recommended that the exercise take place after the BTTR has reached a substantial form. The goal of this exercise is to learn from the testing experience in collaboration with the RTT.

During the replay exercise, the RTT and BT jointly go through the actions that each of the teams has taken during the test, based on the timeline of events agreed to in the reports. They discuss the conducted attack steps and all related issues of interest to allow the BT to gain a deeper understanding of the technical workings behind the actions taken by the RTT and the established or potential future countermeasures.

More specifically, the RTT and the BT shall discuss

- the progression through attack stages of each scenario and the relevant learning generated,
- what else could have been achieved by the RTT with more time and resources,
- potential remediation measures, and
- general questions from the BT.

The findings and learnings of the replay exercise will feed directly into the final Test Summary Report (TSR) and remediation plan.

Required deliverables and meetings

Title	***Responsible party***
Replay exercise	CT
Findings and learnings documented	CT

Required activities

1. The CT shall arrange the replay exercise in the form of workshops or otherwise, with a least the CT, BT and RTT participating.
2. The CT shall have for their records findings and learnings from the replay exercise.

5.5.3 Purple teaming exercise

After the completion of the replay exercise, a PT exercise shall be conducted, in which the RTT and the BT come together to discuss all remaining or additional topics relevant to the CT and the BT. The exercise typically takes the form of one or more workshops.

This exercise is highly beneficial for increasing the learning experience of the entity, anchoring the learnings of the test within the organisation. Potential topics for the PT exercise should be jointly identified by the CT, RTT and the BT and could range from a table-top discussion to technical walkthroughs of the systems.

During the PT exercise, the BT and the RTT further elaborate on the scenarios that have been played out. This exercise allows the stakeholders to discover alternative scenarios and their potential consequences, maximising the learning effect of the overall test.

Although the exercise should be held no later than 10 weeks after the end of the active red team testing, it is highly recommended that the exercise take place after the BTTR has reached a substantial form.

The PT exercise shall cover the requirements and considerations of the TIBER-EU Purple Teaming Guidance (PTG) for the closure phase.

The participants in this exercise are at least the CT, BT and RTT.

Required deliverables and meetings

Title	***Responsible party***
Replay exercise	CT
Findings and learnings documented	CT

Required activities

1. The CT shall arrange the purple teaming exercise in the form of workshops or otherwise.
2. The CT shall have for their records findings and learnings from the purple teaming exercise.

References

- TIBER-EU Purple Teaming Guidance

5.5.4 360° Feedback

After the completion of the replay and PT exercises, the 360° feedback process step takes place. The TM facilitates the 360° feedback process step and is not obliged to provide feedback themselves.

The dedicated 360° feedback meeting, organised by the TM, is focussed on providing feedback to all the stakeholders involved in the testing process. This meeting allows for the participants in the test to reflect upon and improve their approach for future tests. In addition, it also creates the possibility to provide feedback on the testing process as well as the TIBER-FI framework.

The TM may share the output from the 360° 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-FI framework. This is a key part of the "learning and evolving" principle that underlies the TIBER-FI framework.

The key topics to be covered in the 360° feedback output from everyone's perspectives are

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

the participants to this meeting are, at least: the CT, TIP, RTT, BT and TM.

The 360° feedback meeting shall take place before the TM´s approval of the TSR and the remediation plan.

Required deliverables and meetings

Title	***Responsible party***
360° feedback written	CT, TIP, RTT, BT
360° feedback meeting	TM
360° feedback compiled	TM

Required activities

1. The TM shall provide instructions for 360° feedback to the CT, TIP, RTT and BT.
2. The CT, TIP, RTT, and BT shall submit their written feedback.
3. The TM shall facilitate a 360° feedback meeting.

5.5.5 Remediation plan

The remediation plan is, in addition to the replay and PT exercises, also based on the TTIR, BTTR and RTTR. Its aim is to plan improvements and mitigation of vulnerabilities identified during the test.

The remediation plan should be delivered to the TM within eight weeks after the TM has sent a notification of the completed assessment of the RTTR and BTTR. If requested by the TM, a version with sensitive information redacted should be provided instead.

The findings and learnings of the replay and PT exercise will feed directly into the remediation plan.

The remediation plan covers the requirements from the TIBER-EU Remediation Plan Guidance (RPG).

Required deliverables and meetings

Title	***Responsible party***
Remediation plan	Entity

Required activities

1. The entity shall produce a remediation plan and submit it for approval.
2. The TM shall notify the entity of the remediation plan approval.

References

- TIBER-EU Remediation Plan Guidance

5.5.6 Test summary report

The TSR highlights the overall test process and results, and should draw on the test documentation, such as the RTTR, the BTTR, the TTIR as well as the RTTP. Also, findings and learnings of the replay and PT exercise will feed directly into the remediation plan.

The test summary report covers the requirements from the TIBER-EU Test Summary Report Guidance (TSRG).

The entity should be aware of the sensitivity of the TSR. Sensitive, detailed technical information about findings and identified vulnerabilities at a detailed level may cause great risks in the wrong hands.

The TSR should be delivered by the entity to the TM within eight weeks after the TM has sent a notification of the completed assessment of the RTTR and BTTR. The TM shall approve the TSR. If requested by the TM, a version with sensitive information redacted should be provided instead.

Required deliverables and meetings

Title	*Responsible party*
Test summary report	Entity

Required activities

1. The entity shall produce a test summary and submit it for approval.
2. The TM shall notify the entity of the test summary report approval.

References

- TIBER-EU Test Summary Report Guidance

5.5.7 Attestation from Bank of Finland

At the end of the test, once the TM has approved the TSR as well as the remediation plan, the Bank of Finland provides a signed attestation confirming that the test was conducted in accordance with the core requirements of the TIBER-FI framework. The issuing of the attestation concludes the TIBER-FI test.

The attestation covers the requirements and makes use of the template from the TIBER-EU Attestation Guidance (AG).

A TIBER-FI test attestation can serve as a means of qualifying the test for mutual recognition among other authorities. In cases where other TCTs did not participate in the test but there was mutual agreement to share the test results, the entity should share the TSR, the remediation plan and the attestation. The TSR serves as a form of assurance that the test has indeed been conducted, and the attestation qualifies the test as a legitimate TIBER-FI test.

Required activities

1. The Bank of Finland shall issue a signed attestation.

References

- TIBER-EU Attestation Guidance

5.5.8 Sharing the results with the FIN-FSA

Once the entity has the TSR, the remediation plan, and the attestation ready, they must without undue delay share these documents with the Finnish Financial Supervisory Authority (FIN-FSA) as outcomes from a TIBER-FI test.

Required activities

1. The entity shall share the TSR, the remediation plan, and the attestation with the FIN-FSA.

6 Annex 1: Responsibility assignment matrix for a TIBER-FI test

Requirement	Responsible	Accountable	Consulted	Informed	Relevant documents
Preparation phase					
Notification letter	TCT	TCT	FIN-FSA	Management body of the entity	
Assignment of TM	TCT	TCT		TM, Management body of the entity, FIN-FSA	
Appointment of CTL	Management body of the entity	Management body of the entity	TM		TIBER-EU Control Team Guidance
Notification meeting	TM	TCT	CT		TIBER-EU Guidance for Service Provider Procurement
Initiation documents	CTL	Management body of the entity	TM		TIBER-EU Control Team Guidance
Initiation meeting	CTL	Management body of the entity	TM		
Validation Initiation documents	TM	TCT		CTL	
Validation CT composition	TM	TCT		CT	
Procurement process and formal contracts between the different stakeholders	CTL	Management body of the entity	TM (non-objection)	TIP/RTT	TIBER-EU Guidance for Service Provider Procurement
Launch meeting	CTL	Management body of the entity	TM, TIP/RTT		
Scope specification document	CTL	Management body of the entity	TM (FIN-FSA)	TIP/RTT, once available	TIBER-EU Scope Specification Document
Scoping meeting	CTL	Management body of the entity	TM	TIP/RTT, if available	
Validation Scope specification document	TM	TCT	TCT	Management body of the entity	
Risk assessment	CTL	Management body of the entity	TM (non-objection)	TIP/RTT	
Testing phase: threat intelligence					
Scenario selection meeting	CTL, TIP	CT	TM, RTT		
Scenarios created	TIP	CT	TM, RTT		
Targeted Threat Intelligence Meeting	CTL, TIP	CT	TM, RTT		
Targeted Threat Intelligence Report	TIP	CT	TM, RTT		TIBER-EU Targeted Threat Intelligence Report Guidance
Approval Targeted Threat Intelligence Report	TM, CTL	TM, CT		TIP	
Testing phase: red team testing					
Red Team Test Plan	RTT	CTL	CT, TM, TIP		TIBER–EU Red Team Test Plan Guidance
Red Team Test Plan meeting	CTL, RTT	Management body of the entity	CT, TM, TIP		
Approval Red Team Test Plan	TM, CT	TM, CT		RT testers	
Weekly test meetings or updates	CTL, RTT	CTL	TM, TIP, if requested		

Requirement	Responsible	Accountable	Consulted	Informed	Relevant documents
Provision Leg-ups, if necessary	CT	Management body of the entity	RTT, TM		
Closure phase					
Blue Team briefing	CTL	Management body of the entity		BT	
Red Team Test Report	RTT	CTL		BT, TM	TIBER-EU Red Team Test Report Guidance
Blue Team Test Report	BT	CTL	RTT	CT, RTT, TM	TIBER-EU Blue Team Test Report Guidance
Assessment RTTR and BTTR	TM	TM		CT	
Replay exercise	RTT, BT	CTL		TM	
Purple Teaming exercise	RTT, BT, CTL	CTL		TM	TIBER-EU Purple Teaming Guidance
Feedback meeting	CT, RTT, BT, TIP	CTL	TM		
Test Summary Report	CT	Management body of the entity	TIP/RT testers	TM	TIBER–EU Test Summary Report Guidance
Approval Test Summary Report	TM	TM		CT, TCT	
Remediation Plan	CT	Management body of the entity		TM, TCT	
Expert opinion on eligibility for attestation	TM	TM	CT, TIP, RT testers	TCT	
Attestation from BoF	TCT	TCT	TM		TIBER-EU Attestation Guidance
Attestation from FIN-FSA	FIN-FSA	FIN-FSA	TM		TIBER-EU Attestation Guidance