TIBER-BE

Threat Intelligence Based Ethical Red Teaming

TIBER-BE
National Implementation Guide

Version 2.0d
December 2022

Traffic Light Protocol: TLP-White

Table of Contents

List of Abbreviations

APT	Advanced Persistent Threat
BT	Blue Team
CF	Critical Function
CI	Concerned Institution
CISO	Chief Information Security Officer
CEO	Chief Executive Officer
COO	Chief Operational Officer
GTL	Generic Threat Landscape
HUMINT	Human Intelligence
NDA	Non-Disclosure Agreement
NIC	National Implementation Committee
OSINT	Open-Source Intelligence
PII	Personal Identifiable Information
RACI	Responsible Accountable Consulted Informed (RACI-Matrix)
RT	Red team
RTTP	Red Team Test Plan
TCT	TIBER Cyber Team
TECHINT	Technical Intelligence
TI(P)	Threat Intelligence (Provider)
TIBER-BE	Threat Intelligence Based Ethical Red Teaming Belgium
TIBER-EU	Threat Intelligence Based Ethical Red Teaming Europe
TLP	Traffic light Protocol
TPM	TIBER Programme Manager
TTI	Targeted Threat Intelligence
TTM	TIBER Test Manager
TTPs	Tactics, Techniques and Procedures
WT	White Team
WTL	White Team Lead

Change Log

Version	Date	Comments
2.0a	July 2022	Sent to members for feedback
2.0b	October 2022	Member feedback included
2.0c	November 2022	TIBER-EU Secretariat feedback included
2.0d	December 2022	NBB Board of Directors approval for publication

Legal disclaimer and copyright notice

The information and opinions expressed in this document are for information purposes only. They are not intended to constitute legal or other professional advice and should not be relied on or treated as a substitute for specific advice relevant to particular circumstances. The sponsors and authors of this document do not accept any responsibility for any errors, omissions, or misleading statements in this document, or for any loss that may arise from reliance on the information and opinions expressed in it.

This document, the "TIBER-BE national implementation guide", is compliant with and based on the TIBER-EU framework [1]. The NBB has made changes to these materials, to which the NBB owns the copyrights.

Purpose of this guide

This guide has been developed by the TIBER team at the NBB in close cooperation with Concerned Institutions. It is meant to benefit these TIBER-BE participants and their external cyber security service providers. It explains the key phases, activities, deliverables, and interactions involved in a TIBER-BE engagement.

This document is a guide rather than a detailed prescriptive process. It should therefore be consulted alongside other relevant TIBER-BE and TIBER-EU materials which will be provided by the TCT to TIBER-BE participants. The TCT is available to answer any questions that Concerned Institutions or external cybersecurity service providers might have on the methodology, both during as outside a specific engagement. All such questions can be submitted via mail to tiber-be@nbb.be .

1. Introduction

1.1 Background

In its mission to safeguard the stability of the financial system, as stipulated in articles 12, § 1 and 36/33, § 1 of the Law of 22 February 1998 establishing the organic statute of the National Bank of Belgium ("NBB"), the NBB is designated as responsible for detecting, evaluating and monitoring various factors and developments which may affect the stability of the financial system, particularly in terms of affecting the resilience of the financial system or an accumulation of systemic risks. In this respect, the NBB is tasked with, amongst others, monitoring Belgian Critical Market Infrastructures and Core Financial Institutions (further referred to as Concerned Institutions or "CI"), who must remain resilient to cyber-attacks as to avoid a systemic impact of these attacks on the Belgian (and by extension European) financial system. To help achieve this goal, the NBB adopted the TIBER-EU Framework (May 2018) and leads the implementation of the Threat Intelligence-based Ethical Red Teaming [1] framework in Belgium: "TIBER-BE". The Belgian implementation of the TIBER-EU framework involves a joint effort by market participants. Article 13 of the Law of 22 February 1998 allows the NBB to use the TIBER-BE national implementation as a tool to reach the objectives as set out in the Law of 22 February 1998 establishing the organic statute of the National Bank of Belgium described above.

Within the TIBER-BE national implementation, the Concerned Institutions are invited by the NBB to perform, on a voluntary basis, a TIBER-BE assessment by relying on external Threat Intelligence and Red Team providers. These providers respectively identify and simulate the most relevant threats to the concerned institutions' critical economic functions, mimicking attacks by existing highly skilled threat groups. As such, the prevention, detection and response capabilities of the CI against these kinds of attacks are assessed (capability assessment). TIBER-BE engagements are performed following a periodic 3-year cycle and aim to improve the cyber capabilities and cyber resilience of targeted institutions. This supplements the current information security audits (process assessments) performed by e.g. supervisors and overseers. These TIBER-BE capability assessments also complement existing penetration tests and vulnerability scans already performed by the CI. The assessment owner is the CI and is supported by the NBB TIBER-BE Cyber Team (TCT). TIBER-BE should therefore ultimately be seen as a catalyst to enhance the cyber resilience and stability of the financial system as a whole.

1.2 TIBER-BE assessments in a nutshell

Assessments performed under TIBER-BE are "by the CI, for the CI", as the tested institution leads the engagement and directly benefits from the identified improvements. The TIBER-BE Cyber team of the NBB assists, coaches, and supports the institution during the entirety of the engagement. It is important to note that TIBER-BE engagements are rather complex undertakings, involving multiple stakeholders and spanning over several months, requiring thorough planning and coordination between all participants of the engagement.

The bulk of the preparation and planning of these assessments is done by the White Team ("WT"), this is a select group of employees of the CI that are aware a TIBER-BE assessment is taking place. The WT is normally limited in size and consists of security and business experts, including a representative of the CI's board. It is characteristic of a TIBER-BE engagement that any employees outside the WT are not aware a test is taking place, in order not to influence the behaviour of the CI's personnel. The WT is responsible for the preparation and coordination of the engagement. During the test, The WT will monitor the testing progress and intervene when deemed necessary, e.g. to avoid critical impact on live production systems or external escalations. The WT will be assisted in its efforts by the NBB TIBER-BE Cyber Team ("TCT"). The TCT consists of a Programme manager and one or more Test managers. The main responsibility of the TCT is assisting the WT as well as

[1] Another generic term used in the literature is Threat Led Penetration Testing (TLPT)

other participants involved in a TIBER-BE assessment, while making sure all requirements of the TIBER-BE national implementation are met.

TIBER-BE tests adhere to well-defined scenarios produced by an external threat intelligence ("TI") provider and based on a commercially obtained "Generic Threat Landscape" ("GTL") document, describing, amongst others, the threat landscape for the Belgian financial sector. The external threat intelligence provider enriches the information from this GTL document with intelligence relevant to the tested CI, leading to scenarios specifically simulating the most relevant threat actors and targeting the most relevant critical economic functions of the CI in scope. A TIBER-BE test can therefore be defined as the highest possible level of intelligence-based Red Teaming exercise, using the same Tactics, Techniques and Procedures ("TTPs") as real adversaries, against live critical production infrastructure. The actual execution of the developed scenarios, the actual testing activities in a TIBER-BE assessment are performed by an external Red Team ("RT") provider. Scenarios are executed without the prior knowledge of the organisation's defending Blue Team ("BT") to mimic a real attack as accurately as possible. The active part of the engagement consists of time-boxed phases (reconnaissance, in, through, and out). This allows for a thorough evaluation of the existing prevention, detection, and response capabilities against advanced attacks. It also helps identify weaknesses, vulnerabilities, or other security issues in a controlled manner. After scenarios are fully executed or in case the Red Team were to be detected during the scenario execution and covert continuation of the test would be no longer possible, a more collaborative mode of testing (Purple Teaming) can be adopted where Red Team and Blue Team work together to continue the test. Such a Purple Teaming approach, however, can only be started in consultation and agreement with the TCT.

Once the Red Team phase is completed, the engagement moves to the closure phase**.** In this phase, a replay of the test is performed where the RT and BT convene and go through the activities performed during the test. The goal of this replay is to understand the findings, identify and address any additional gaps in the security controls, and improve the overall cyber defence and response capabilities of the CI. The closure phase also covers the reporting activities by the Red Team, the Blue Team and the White Team.

Collaboration, trust, and improvement lie at the heart of TIBER. What differentiates TIBER-EU from other security testing frameworks is its intelligence-led ("actors", their "capabilities" and "intent" in threat intelligence terminology), holistic, and live systems testing approach. This means that Concerned Institutions can improve their resilience based on proven relevant weaknesses rather than on perceived / theoretical weaknesses. By using the TIBER framework, a higher return on security investments can be obtained than by solely working with a compliance-driven risk framework. In addition, the central role of the TCT enables aggregation of test results within the TIBER-BE community and the distillation of best practices for the entire sector.

1.3 Responsibilities and liability

Each participant in a TIBER-BE engagement is exclusively responsible and liable for the execution of the tasks attributed to them by this framework, including compliance with applicable laws and regulations. It is their responsibility to conduct a review of applicable laws and regulations, both national, international and of the different involved jurisdictions to ensure that the execution of the tasks attributed to them does not infringe any such law or regulation and to take appropriate risk management measures (e.g. make relevant contractual arrangements) to enforce compliance and ensure operational risks of the engagement are under control. The risks considered in this risk management exercise should not be limited to operational aspects directly related to the Red Teaming phase, but also cover business continuity, brand image, reputation, confidentiality, and financial risks among others. When exchanging TIBER-BE related documents, the TCT refrains from receiving and processing any documents containing IP or PII of the individuals targeted or identified during the engagement. Any documents and reports submitted to the TCT should therefore be reviewed and redacted where necessary before submission.

Unless explicitly agreed otherwise, the tested institution bears the costs and expenses for participating in a TIBER-engagement.

2. TIBER-BE overview

2.1 Introduction

This section provides an overview of the TIBER-BE engagement phases and the roles and responsibilities of each of the different stakeholders.

2.2 Stakeholders

When considering the stakeholders relevant to the TIBER-BE implementation, a distinction must be made between the stakeholders in the TIBER-BE national implementation and the participants in a specific TIBER-BE engagement. While there is an overlap between both groups, the roles and responsibilities of stakeholders in the TIBER-BE national implementation and participants in a TIBER-BE engagement differ significantly.

2.2.1 The TIBER-BE Team

The TIBER-BE Team is the team at the NBB responsible for maintaining the national implementation guide itself, updating TIBER-BE documentation and inform relevant stakeholders of any evolutions. The cyber security sector and cyber threat landscape are part of an ever-changing environment, and it is essential that TIBER-BE evolves along with the sector to remain relevant and maximise the value for all concerned institutions tested. As TIBER-BE is a national implementation of the European TIBER-EU framework, this requires the TIBER-BE team to liaise closely with other TIBER-XX implementations and the TIBER-EU team to ensure any changes to the TIBER-BE national implementation guide are in accordance with TIBER-EU and vice versa. Besides maintaining the national implementation guide, the TIBER-BE Team is also involved in the execution of a TIBER-BE engagement. The exact role of the TIBER-BE Team in a specific TIBER-BE engagement is explained further below.

The NBB's TIBER-BE Team consists of a TIBER-BE Programme Manager ("TPM") and a number of TIBER-BE test Managers ("TTM"). The programme manager coordinates the governance activities overarching the different TIBER-BE engagements, transversal activities and (inter-)national fora and committees in which the TIBER-BE team is active. The TPM is also the first escalation point in case of an issue or incident related to a specific engagement, and thus is kept informed of the status and evolution of the different engagements by the test managers who are, in turn, responsible for the operational follow-up of the engagements and guidance of the different participants involved. The test managers are also key to translating their experience into improvements for the TIBER-BE national implementation.

Although the TIBER-BE Team is employed by the NBB, the team does not operate in a supervision nor oversight capacity. Instead, the TIBER-BE national implementation and consequently the TIBER-BE Team is in line with financial stability mission (cfr 1.1) and is implemented as a catalyst, working alongside the industry to improve the resilience and capabilities of the Belgian financial sector. Because of this catalyst role, there is no legal obligation for institutions to participate in a TIBER-BE engagement. All TIBER-BE engagements are executed on a voluntary basis. This arrangement facilitates collaboration and trust between participants, which are key success factors of a TIBER-BE engagement and the TIBER-BE national implementation.

2.2.2 The TIBER-BE community and the National Implementation Committee (NIC)

To facilitate transparency and alignment between the different institutions in scope of the TIBER-BE programme, a TIBER-BE community was established at the same time the framework was implemented. The TIBER-BE community is a trusted group of institutions, within which the participants can share their TIBER-BE experience, lessons learnt and experiences from performing a TIBER-BE engagement and other best practices in cyber and IT security. Furthermore, the community is also invited to provide feedback on the national implementation and can propose improvements to the framework to increase the benefit derived from TIBER engagements. The TIBER-BE community consists of:

- **All institutions in scope of the TIBER-BE national implementation**: The scope of the TIBER-BE national implementation was defined in line with the financial stability mission of the NBB, including all critical financial institutions and critical market infrastructures operating in Belgium. The initial TIBER-BE scope was defined at the start of the first cycle of TIBER-BE assessments; however, it is extended as TIBER-BE evolves.
- **The TIBER-BE team**: The TIBER-BE programme manager and all TIBER-BE test managers.

Most of the information sharing between the members of the TIBER-BE community occurs on the TIBER-BE National Implementation Committee (NIC), a biannual meeting, chaired by the NBB, assembling all stakeholders relevant to the TIBER-BE implementation. Besides the members of the TIBER-BE community, the NIC also includes several observers and allows for the invitation of experts to present and discuss specific cyber security topics:

- **The TIBER-BE threat intelligence provider:** The Threat Intelligence Provider procured by the TIBER-BE community to produce the Generic Threat Landscape document will also provide a high-level overview of the threat landscape on each TIBER-BE NIC meeting. The threat intelligence provider also updates the TIBER-BE community on relevant evolutions in the threat landscape through a dedicated communication channel.
- **The Belgian Intelligence Agencies:** The Belgian intelligence agencies enrich the information provided by the Threat Intelligence provider and present their view on the current state of the Cyber Threat landscape.

2.2.3 The participants in a TIBER-BE engagement

At the core of the TIBER-BE implementation are the threat-led penetration tests performed on a regular basis with each of the financial institutions in the scope of TIBER-BE. The stakeholders involved in performing a TIBER-BE engagement are:

- **The Concerned Institution (CI):** The financial institution undergoing the TIBER-BE assessment
    - The White Team: This team, led by the White Team Lead (WTL), is aware of the test and will be responsible for the coordination.
    - The Blue Team: This team is responsible for defending the institution against potential attackers and is therefore not aware a test is taking place.
- **The external providers**:
    - Threat Intelligence provider
    - Red Team provider
- **The TIBER-BE Cyber Team (TCT):** The members of the TIBER-BE Team that will be actively involved in the test, this includes one or more TIBER-BE test managers and the TIBER-BE program manager.
- **Other relevant authorities:** In case of multi-jurisdictional exercises, the Concerned Institution together with the TCT agree which authorities are to be involved in the engagement, how they are involved and in what capacity, depending on the coverage and location of the critical functions (CFs). In general, multi-jurisdictional exercises are initiated

and driven by the lead supervising or overseeing authority. If another authority seeks to initiate and lead the engagement, the lead supervising or overseeing authority must first agree to this.

Of these listed stakeholders, the Concerned Institution's White Team will be the primary responsible for planning and coordinating the TIBER-BE engagement. However, to assist the White Team in its efforts, the NBB provides experts in cyber security and in the TIBER process, the TIBER-BE Cyber team ("TCT").

The main role of the TCT is to make sure Concerned Institutions undergo tests in a uniform and controlled manner, meeting all requirements of the TIBER-BE national implementation. To achieve this, the TCT cooperates closely with the WT during all phases of the TIBER-BE process. The TCT convoys the WT through the TIBER-BE phases but can in no way be held accountable or liable for the WT's actions or for any consequences of the TIBER-BE engagement for the participating Concerned Institution or third parties. Despite its close relationship with the WT, the TCT is not formally part of the WT. The TCT has a right to escalate (major) deviations from the TIBER-BE methodology or spirit to the person to whom s/he directly reports or/and to the Concerned Institution's Executive member like CEO, COO or CISO. Escalation should, however, be a last resort.

2.3 Process overview

2.3.1. Pre-test arrangements

Before any testing under TIBER-BE can commence, some important preparatory work must be carried out. One of the most important elements in preparing the engagement, is the development and distribution of a Generic Threat Landscape ("GTL") document. This document is issued by the TIBER-BE threat intelligence provider and distributed to all TIBER-BE National Implementation Committee members and observers. It provides an overview of the cyber threat landscape for the Belgian financial system. It serves as an input for the Threat Intelligence phase of a TIBER-BE and can therefore not be omitted from the TIBER-BE process. Furthermore, because the GTL contains general information relevant to all members of the TIBER-BE community, the applicability of this document is not limited to TIBER-BE engagements as it can also be used as input for other risk management processes. The GTL document is updated twice each year and can thus be used in several engagements. As such, generic threat intelligence collection cannot be considered to be part of any specific TIBER-BE engagement.

2.3.2. Phases of a TIBER-BE engagement

The TIBER-BE process consists of four distinct phases:

1. During the **Preparation Phase,** the TIBER-BE engagement is formally launched, the WT is established, the scope is determined. A RT provider and a TI provider are procured.
2. During the **Threat Intelligence Phase,** the threat intelligence provider drafts the scenarios to be executed in the Red Teaming phase of the engagement. Scenarios are based on the Generic threat landscape document, enriched with specific intelligence about the CI targeted in the test.
3. The **Red Teaming Phase** is the active part of a TIBER-BE engagement. In this phase, the Red Team provider executes the scenarios developed by the TI provider in order to assess the CI's cyber capabilities.
4. In the **Closure Phase,** the TIBER-BE engagement is wrapped up. The RT and BT convene and go through the different techniques used in the Red Teaming phase; this is called the replay workshop. Another important aspect of the closure phase is the writing of several reports required by the TIBER-BE national implementation. The BT, RT and WT deliver their reports, discussing the findings encountered during the Threat Intelligence and Red Team phases. The test summary report, produced by the WT, also contains a high-level

remediation plan. The last steps of the engagement are the organisation of a 360° feedback session and providing the TIBER-BE attestation for mutual recognition.

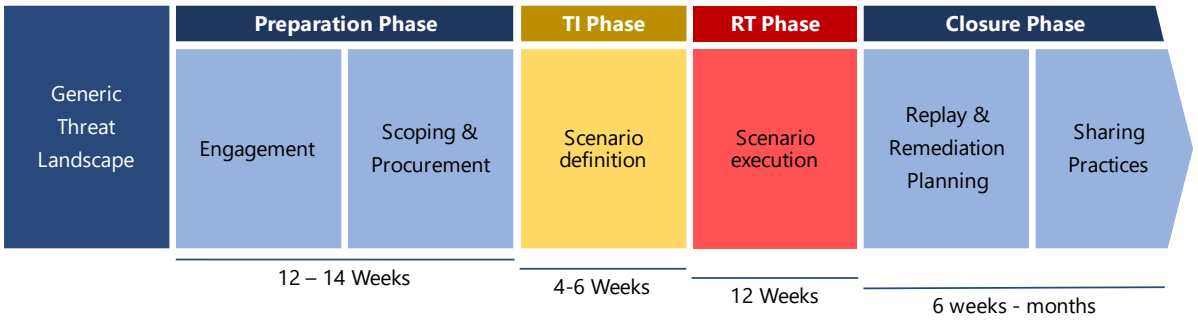

Figure 1 TIBER-BE process overview

2.3.3 Role of the TCT and White Team

The responsibility for the overall planning of a TIBER-BE engagement lies with the Concerned Institutions. The WT in the Concerned Institutions coordinates all activities, including engagement with the service provider(s). The TCT does not maintain a list of "approved" or "accredited" service providers or give market procurement advice. The role of the TCT in the procurement phase is to ensure that the providers selected by the CI meet the minimum requirements set out in the TIBER-EU Service Procurement guidelines[1].

Service provider(s) produce an activity planning for the Concerned Institution to factor into the overall TIBER-BE project planning. Significant deviations in the original planning will be discussed with the TCT. The TCT has direct access to the service providers when needed.

The TCT, after consulting the relevant supervision/oversight colleagues at the NBB, validates that the scope is sufficiently detailed for the test to begin. The TCT will also provide feedback on the scenarios to ensure that the test is executed according to plan and up to the TIBER-BE standards. While there must be close cooperation between the TCT and the WT, individual roles and responsibilities should be respected. When crucial decisions need to be made or in case unclarities or diverging opinions emerge, the TPM will be involved. This includes for example deviations from the agreed scope.

The TCT may in rare cases invalidate the TIBER-BE engagement where the performance, quality or secrecy of the test is compromised, e.g. in case:

- the TI provider or the RT provider has repeatedly shown it does not or cannot comply with the requirements or standards laid out in the TIBER-BE national implementation guide;
- the test has been compromised by the RT provider, the TI provider or the Concerned Institution either fraudulently, intentionally or as a result of gross negligence.

The TCT will take this decision in consultation with the WT, unless the circumstances do not, in the opinion of the TCT, allow for this. The TCT will communicate the reasons for its decision to the involved parties. The removal of the TIBER-BE label implies that the test is not recognized as a TIBER-BE engagement. This means that, in case of a multi-jurisdiction test, the test will not be recognised as a TIBER-XX test in other jurisdictions or, in case of a national test, will not be taken into account for the multi-year cycle of TIBER-BE engagements.

TIBER-BE engagements should be a learning experience and should thus be underpinned by a collaborative, transparent, fair, ethical, and flexible working approach by all parties involved.

[1] https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html

2.4 Managing the risks involved during the test

Due to the criticality of the target systems, the people and the processes involved, an inherent risk can be associated with performing a TIBER-BE assessment. Therefore, prior to commencing any active testing, the WT is required to conduct an in-depth risk assessment followed by the implementation of all the necessary risk mitigating controls, processes, and procedures to ensure a controlled test.

To further limit the risks incurred when conducting a TIBER-BE assessment, the TIBER-BE national implementation has included several provisions prohibiting specific testing activities. These activities are, among others:

- destruction of equipment;
- uncontrolled modification of data / programs;
- jeopardising continuity of critical services;
- extortion;
- threatening or bribing employees;
- disclosure of results

Other activities performed by the RT must of course be in accordance with the applicable legislation and the rules of engagement agreed upon by all participants.

3. Generic Threat Landscape

One of the key success factors of a TIBER-BE assessment is the threat intelligence on which the executed scenarios are based. Solid threat intelligence allows for the identification of most relevant threats and threat actors. By translating this intelligence into clear, actionable scenarios, the TIBER-BE testing methodology ensures that those systems, that are at the highest risk of being exploited by real threat actors, are thoroughly assessed, focussing the lessons learned from a test to the areas that matter. Furthermore, the value of thorough threat intelligence goes far beyond the TIBER-BE assessment in which it is used. The intelligence can serve as input for the CI to identify relevant risks and optimise specific security controls as well as the institution's overall security posture.

To aid the threat intelligence efforts related to an engagement, the TIBER-BE implementation includes a provision for a generic threat landscape document (GTL). The GTL is a document describing the threat landscape for the Belgian financial sector, more specifically, for the financial institutions in scope of the TIBER-BE implementation. The document is produced by a third-party threat intelligence provider commercially procured by the TIBER-BE community and updated twice a year. It is shared prior to the start of the Threat Intelligence phase of each TIBER-BE assessment with the CI and the procured providers. It forms the basis for the Targeted Threat Intelligence report.

4. Preparation Phase

4.1 Overview

During the TIBER-BE Preparation Phase, the engagement is formally launched. The scope is established, and the Concerned Institution procures the service provider(s). The duration of the preparation phase is mainly governed by the duration of the procurement process. This differs between CIs but can generally take up to 14 weeks.

Relevant documents for this phase are:

- TIBER-EU White Team Guidance;
- TIBER-EU Services Procurement Guidelines;

- Scope Specification Guidelines and attestation Templates;
- Risk Management Guidelines;

Outputs of this activity are:

- Establishment of the Concerned Institution's White Team and identification of all stakeholders by the Concerned Institutions;
- List of the service providers procured by the Concerned Institutions;
- Analysis produced by the concerned institutions, checking the compliance to the TIBER-EU Services Procurement Guidelines for both of the procured service providers;
- Scope Specifications produced by the Concerned Institutions for delivery to the TCT and service providers;
- Scope attestation signed by a senior executive or board member;
- Risk management documentation produced by the Concerned Institutions for delivery to the TCT and service provider(s);
- Project Planning produced by the Concerned Institutions for delivery to the TCT and aligned with the service provider(s).

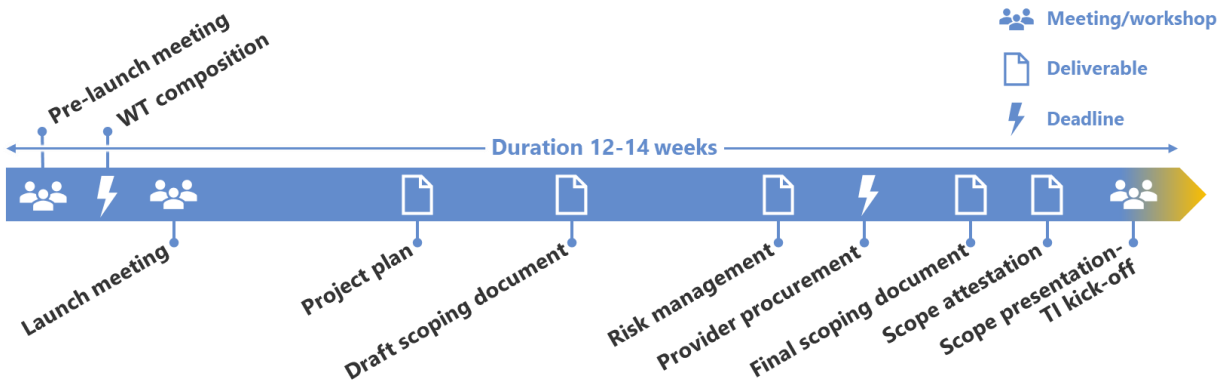

Figure 2 Timeline of the TIBER-BE preparation phase

4.2 Stakeholder identification and White Team composition

The pre-launch meeting marks the start of the TIBER-BE process and serves as the first contact between the TCT and the concerned institution. In this meeting, the designated contact person for TIBER-BE at the CI[1] is consulted to discuss when a TIBER-BE engagement can be planned. The TCT requests the CI to appoint a White Team lead and start assembling a WT according to the TIBER-EU White Team Guidance[2]. Any other relevant stakeholders that should be involved in the engagement are also identified in consultation with the CI. Once the White Team is established, a launch meeting is organised, where the TCT gives a detailed explanation on the TIBER-BE process and requirements. During the launch meeting, the WT and TCT will also agree on a code name for the tested institution. Given the sensitive nature of a TIBER-BE engagement, this code name is to be used by all stakeholders.

Following the pre-launch and launch meetings, regular status update meetings between the TCT and the WT are held to check in on the preparation progress and to assist the WT where needed.

4.2.1 White Team

As previously stated, the WT is responsible for the planning and coordination of the TIBER-BE engagement. In the preparation phase, the WT is tasked with the creation of the project plan, the

[1] When the TIBER-BE framework was first established, a contact person for each CI was identified. These are often the representatives of the institution in the TIBER-BE community and the NIC
[2] https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html

procurement of the external providers, the definition of the scope and drafting the risk management document. Throughout the engagement, the WT will be in close contact with the providers and the TIBER-BE Cyber Team, ensuring all TIBER-BE requirements are met and the test is executed in a controlled manner. The WT is also responsible for intercepting and containing any escalation by the BT related to the testing activities.

The WT should consist of the minimum number of people required to meet all expectations formulated in the TIBER-BE national implementation guide (i.e. sufficient knowledge of the systems in scope, able to intercept all escalations originating from the test and a board representative, able to assist the RT where necessary). Typically, the WT consist of one White Team Lead and three to four security, risk or IT experts but this depends on the institution being tested. During the execution of the engagement, it can become desirable to extend the WT with additional subject matter experts ("SMEs") or other employees that have specific role or knowledge. The WT lead should also carefully consider if specific key functions (SOC leader, IT risk manager, 2nd line of defence …) needs to be part of the test, thus be in the BT, or on the contrary be part of the WT.

Under the TIBER-EU framework, the ECB has published a *TIBER-EU White Team Guidance* document [2] which aims to assist the target institution in establishing a capable White Team.

4.2.2 Other stakeholders

In some cases, the CI being tested is active on an international level and would prefer to include its operations and/or infrastructure outside the Belgian territory in the scope of the test. This is certainly encouraged under TIBER-BE as it allows for a more complete test coverage of the concerned institution. Where and when applicable, the national competent authorities of the involved countries should be informed of the test. If one of these involved national authorities has its own TIBER-XX implementation or a similar framework for performing threat-intelligence-based tests[1], the possibility of a joint test can be explored. In a joint test, multiple TCTs/regulators will be involved in the assessment. In practice one TCT, generally the TCT linked to the CI's lead overseer, will be designated as main point of contact to limit the amount of additional effort such a joint test brings to the CI.

A more detailed guidance on how multi-jurisdictional testing is organized can be found in the TIBER-EU Framework [1].

4.3 Preparation phase core deliverables

After the launch meeting, the preparation for the upcoming TIBER-BE engagement begins. The WTL and other WT members appointed in the launch meeting receive documentation from the TCT describing the TIBER-BE process and TIBER-BE requirements. Besides the establishment of the WT, the preparation phase consists of four distinct aspects: the creation of a high-level project plan, the procurement of the providers, the specification of the scope and a risk management analysis. Throughout the preparation phase, regular calls can be held between the TCT and the WT to follow-up on the progress and to aid where necessary.

4.3.1 High-level project plan

Once the White Team is established and all relevant stakeholders (e.g. other relevant authorities) are identified, a project plan can be drafted and submitted to the TCT. In the project plan, general agreements are recorded, the different WT members, WTL and other stakeholders are identified, and a preliminary, high-level planning is provided. This document will help as a guideline for future communication and interaction between stakeholders and as a gauge to verify whether the engagement is on track.

[1] Such as test performed under the CBEST framework implemented by the Bank of England [3] or Thread-led penetration tests (TLPT) as described in the European Digital Operational Resilience Act (DORA) [4]

4.3.2 Provider procurement

After the launch meeting, the Concerned Institution starts its procurement process and selects an external RT Provider and TI Provider that will be tasked with performing the test. Once a first preselection of providers has occurred, a shortlist can be provided to the TCT. The TCT will in turn verify the compliance of the selected providers with the TIBER-EU Service Procurement Guidelines [5]. The TCT will not impose a specific provider to the institution, and, in the absence of strong objections against one or more of the providers on the shortlist, it remains at the Concerned Institution's discretion to decide which provider it wishes to procure and the CI is fully responsible for the choice of the providers.

During the procurement process, the Concerned Institution:

- ensures that it has the necessary NDAs in place with the involved service providers;
- procures and onboards a TI provider and an RT provider in respect of the TIBER-EU Services Procurement Guidelines;

4.3.3 Scope definition

During the launch, the TCT provides the Concerned Institution with Scope Specification guidelines. The Concerned Institution then starts working on a draft version of the Scope Specification, with the aim to identify and include all Critical Functions ("CFs") carried out by the CI. Critical Functions are defined as the people, processes and technologies required to deliver a core service which, if disrupted, could have a detrimental impact on the financial stability, the Concerned Institution's safety and soundness or the institution's customer base.

Note that a CF is not a specific IT system, it is a business function. Concerned Institutions across the sector support and deliver these functions in different ways via their own internal processes, which are in turn underpinned by critical IT systems. These critical technologies, processes, and the people surrounding them, are the focus of TIBER-BE threat intelligence and Red Teaming. This can include any of the third-party service providers delivering services to CI related to its identified critical functions (Critical Third-Party Providers or CTPPs). If a CTTP is included in the scope of the TIBER-BE engagement, it might be necessary to foresee representation of the CTTP in the WT.

Besides the requirement to include all critical functions and underlying critical systems, the WT can choose to include other, less critical systems in the scope of the assessment. As such, the WT can identify systems it deems interesting targets despite their less critical nature.

Once identified, flags can be defined for each of the CFs in the scoping document. These flags are the goals for the later test scenarios which are based on relevant threat intelligence. The WT should discuss the flags with the TCT, who must approve them. The Concerned Institution can choose to involve the RT provider and TI provider in the scoping process. The TCT is available during the scoping process to clarify the requirements and give feedback.

4.3.4 Risk management

Prior to conducting the test, the WT conducts a risk assessment to ensure all the necessary risk management controls, processes, and procedures for a controlled test are in place. These risks include, but are not limited to:

- Legal and provider risks
- Reputational and ethical risks
- Crisis and incident escalation
- Operational Red Teaming risks
- Operational Blue Teaming risks

- Clean-up related risks
- General project risks

To assist the WT in its efforts to identify and mitigate the risks incurred during a TIBER-BE engagement, a Risk Management Template is provided by the TCT. This is a document listing the most important risks and suggestions on possible mitigating actions. However, the risk management template does not contain an exhaustive list of all risks and mitigating actions and the WT is encouraged to complement this document based on the CI's own risk management procedures. While a complete risk management document should be drafted before the kick-off of the TI phase, the risk management document is considered a living document and can be extended in the course of the assessment. Throughout a TIBER-BE engagement, new potential risks can be identified and these risks, together with appropriate mitigating actions, should be added to the risk management document.

4.4 Scope attestation

When a preliminary scope is defined, the WT should deliver a draft scoping document to the TCT for review. The TCT will in turn review this draft scoping document and provide the CI with feedback. As the TCT has limited insight and knowledge of the internal operations of the CI, the team will consult the relevant supervision/oversight authorities when reviewing the draft scoping document. These colleagues are only consulted to verify the scope delivered by the WT is complete and they will in no way be involved in the remainder of the TIBER-BE engagement.

Once the feedback of the TCT is incorporated, the scoping document can be finalised. Before presenting the scope to the TI provider or any other stakeholders, however, a scope attestation document must be signed by a board member of the CI[1]. This board member will serve as the sponsor of the TIBER-BE engagement and ensures board awareness and buy-in for the engagement and the remediation of any findings that may occur during the assessment.

4.5 Scope presentation and TI kick-off

Once all preparations for the TIBER-BE engagement are finished and the scope is signed-off, the WT will organise a meeting with all stakeholders involved in the engagement, i.e., WT, TCT and provider(s). It is encouraged that the board member sponsoring the engagement is also present in this meeting. The goal of this meeting is to provide all stakeholders with an overview of the preparatory steps taken so far and the planning for the remainder of the TIBER-BE engagement. The topics generally handled during this scope presentation are listed below. The WT is invited to add topics to the agenda as they see fit:

- Introduction + roundtable
- Presentation of the scope of the assessment (WT)
- Presentation of the project plan (WT)
- Presentation of the risk mitigations and communication/escalation lines in place (WT)
- Presentation of the TIBER-BE process and TIBER-BE expectations (TCT)
- Presentation of the Threat Intelligence approach (TI provider)
- Presentation of the Red Team approach (RT provider)

After the scope presentation meeting, the WT delivers the completed and signed-off scoping document to the TI provider who can in turn kick-off their threat intelligence efforts. If necessary, an additional TI kick-off meeting can be set up between the TI provider and the WT to answer any questions the TI provider might have on the scope of the assessment. Such a kick-off meeting can be useful to share more detailed information than contained in the scoping document, such as IP ranges and domain names used by the CI and in scope of the assessment.

[1] The TIBER-EU White Team Guidance requires at least one of the members of the CI's board to be part of the WT.

5. Threat Intelligence Phase

5.1 Overview

During this phase, target intelligence is collected in a passive manner by an external threat intelligence provider procured by the WT and threat actor mapping is performed. Based on this intelligence, the provider proposes the attack scenarios that will form the basis for the Red Teaming phase. The main goal of this phase is for the threat intelligence provider to deliver a report containing all intelligence useful to the Red Team. As the Red Team might have additional intelligence requests upon receiving the TI document or during the RT testing, it is encouraged that the TI provider remains available throughout the duration of the engagement.

The threat intelligence phase consists of three main parts:

- Targeted Intelligence collection
- Threat Actor mapping
- Scenario definition

The Threat Intelligence provider can choose whether it delivers these elements as separate reports, or combines them in a single Targeted Threat Intelligence report.

Relevant documentation:

- Scoping document
- Generic Threat intelligence document.
- TIBER-EU guidance for the Target Threat Intelligence report [6]
- Intelligence collection Input for the TI provider (provided by WT)

Output of this phase:

- Targeted Threat Intelligence (TTI) Report(s)

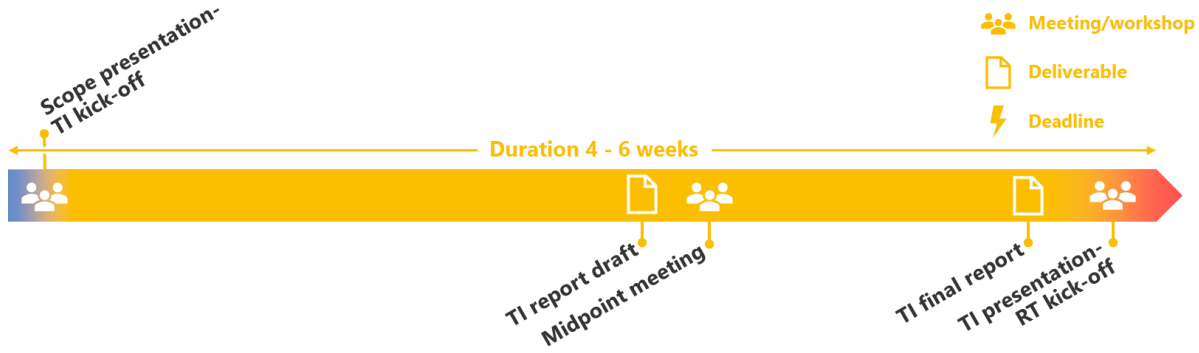

Figure 3 Timeline of the TIBER-BE threat intelligence phase

5.2 Targeted Intelligence Collection

In this phase, the TI provider executes an initial, furtive, broad, and intelligence-based targeting exercise of the kind typically undertaken by threat actors as they prepare for their campaign.

Active reconnaissance on the Concerned Institution is not part of the Targeted Threat Intelligence phase as to minimise the risk of detection before the Red Team phase is even started. The focus is therefore on stealth, using passive reconnaissance techniques (i.e. without direct interaction and impact to the CI people, processes and technologies) with the objective to draw a picture of the Concerned Institution as a target from the attacker's perspective.

The main input for this part of the Threat Intelligence phase is the scoping document drafted by the Concerned Institution's WT, defining the Critical Functions and underlying systems that will be the target of the TIBER-BE engagement. Besides this scoping information, the use of various methods (including OSINT[1], TECHINT[2], HUMINT[3] and intelligence-based initial targeting) is encouraged.

After receiving the scoping document, the TI provider is expected to request additional information from the CI to assist intelligence collection and avoid going out of scope. This can for instance be a list of domains or IPs in scope[3] but can also be additional information regarding business processes and entities in scope (offices, data centres, group companies, specific geographies, etc.)

The output of the Target Intelligence identifies the people, processes, technology, and infrastructure of the Concerned Institution on a Critical Function-focused system-by-system basis, including any critical third-party providers supporting these critical functions. This includes information that is intentionally published by or about the institution, as well as internal information that has been deliberately or unintentionally leaked. This can include customer data, confidential material, identified vulnerabilities or other information that could prove to be useful for an attacker.

5.3 Threat actor mapping

In this part of the Threat Intelligence phase, the different malicious cyber actors posing a threat to the targeted institution will be investigated and categorized. The TI provider will identify the threat actors most relevant to the Concerned Institution and map the tactics, techniques and procedures attributed to these threat actors. This threat intelligence work builds on the Generic Threat Landscape document that is given to the TI provider at the start of the threat intelligence phase. The TI provider is expected to enrich the information provided in the GTL document with own insights and the intelligence collected in the Targeted Intelligence collection phase to produce a contextualized report representing the targeted threat landscape for the CI and its critical functions.

5.4 Scenarios

5.4.1 Threat Intelligence based scenarios

Once a thorough investigation of the threat landscape is performed, the TI provider will combine target- and threat intelligence to develop several realistic scenarios. These scenarios are specifically tailored to the CI and aim to emulate the threat actors posing the greatest threat to the institution. For each scenario, the TI provider will define the narrative, the likelihood, the impacted Critical Function and supporting systems, corresponding flags, the involved threat actor to be emulated, the TTPs used by the selected threat actor, the potential impact on the financial sector, etc.

The TI provider is also expected to include any of the identified target intelligence that could make scenarios even more tailored to the CI or be useful to the Red Team when executing them. The narrative of the scenarios should not limit the creativity of the RT too much as real Threat Actors demonstrate flexibility and also adapt their TTPs in an opportunistic manner. As such, we rely on the professional judgement of the RT and TI providers to suggest alternative TTPs that the RT could use (provided the emulated Threat Actor is deemed to possess the ability to use these TTPs) in case of issues identified or anticipated with the TTPs prescribed in the scenarios.

Under the TIBER-BE national implementation, the TI provider is encouraged to include a physical breach scenario. In such a scenario, the Red Team would be expected to bypass the on-premises physical security measures (e.g. by means of social engineering) to achieve a specific goal described in the scenario (e.g. install a malicious implant, steal confidential information, …). A physical breach

[1] Open Source Intelligence.
[2] Technical Intelligence.
[3] Human Intelligence.
[3] This can already be prepared by the WT in advance to speed up the target intelligence process.

scenario is, however, optional and it can be decided by the WT to exclude it from the proposed scenarios in agreement with the TCT.

Once the TI provider has a first draft of the scenarios it plans to include in the TTI report, a TI midpoint workshop is organised. During the workshop, the TI provider will present the different relevant scenarios it has identified and request input from the different participants in the engagement.

5.4.2 Scenario X

The core of a TIBER-BE engagement is the emulation of real threat actors by using known and observed TTPs to attack the Concerned Institution following well-defined scenarios. While this approach is ideal to detect gaps in security controls that pose a real threat to the institution (i.e., the identified vulnerabilities are at risk of being attacked by the emulated threat actor), it also limits the number of findings that could be detected to the vulnerabilities relevant for the pre-defined scenarios. Furthermore, given that only known and observed TTPs are used in the threat intelligence-based scenarios, more mature institutions have often already mitigated the vulnerabilities, rendering the emulated TTPs ineffective. This could lead to a limited number of findings or detection of the Red Team in the early stages of a scenario. The concept of scenario X has been introduced in TIBER-BE as an answer to this challenge.

Scenario X is a scenario that allows thinking outside of the box. As such, a scenario can be created using innovative TTPs, with a higher chance of uncovering new findings and improvement opportunities. Normally, Scenario X is only defined during the Red Teaming phase, once the RT is somewhat familiar with the CI's infrastructure. However, during the TI phase, the TI provider is encouraged to make suggestions on what TTPs could be considered. The WT is also consulted when preparing for scenario X. The WT could, for example, indicate what TTPs they would like to see tested or what part of the CI's infrastructure could be targeted during this scenario.

Scenario X is a concept specific to the Belgian implementation of the TIBER-EU framework and is therefore not described in the TIBER-EU Guidance for the Target Threat Intelligence Report [6].

5.5 Handover

At the end of the Threat Intelligence phase, once a draft version of the TTI report is available, a final TI meeting will be organised. During this meeting, the Threat intelligence provider will present the TTI report to the White Team, the TCT and the Red Team enabling them to give feedback and requesting some final adaptions of the report.

Once the TI provider has incorporated any feedback of the different participants and delivers the final TTI report, the engagement can officially move into the Red Teaming phase. To facilitate the accurate execution of the prescribed scenarios, it is encouraged that the TI provider remains available to advise the Red Team throughout the Red Teaming phase, possibly even participating in the weekly update call organised during this phase. Participation of the TI provider in the Red Teaming phase allows for further support in case the Red Team has specific questions about the Threat actor emulated during the RT activities.

6. Red Teaming Phase

6.1 Overview

In the Red Teaming phase, the Targeted Threat Intelligence Report is handed over to the Red Team. Before any testing can begin, a Red Team test plan is prepared by the Red Team provider. This plan builds on the proposed scenarios in the TTI report and details the approach the RT will take when executing them. When the RT test plan is finalised and approved, the actual testing can begin. During the test, the RT provider will aim to perform a stealthy intelligence-led Red Teaming exercise against the targeted systems in the CI's infrastructure. The RT Test takes approximately twelve weeks, or longer if felt necessary.

Relevant documentation:

- Targeted Threat Intelligence report
- TIBER-EU Guidance for the Red Team Test Plan [7]
- Red Team status update guidelines
- TIBER-EU Guidance for the Red Team Test Report [8]

Output of this phase:

- Red Team Test Plan
- Red Team Updates
- Red Team Report (draft)

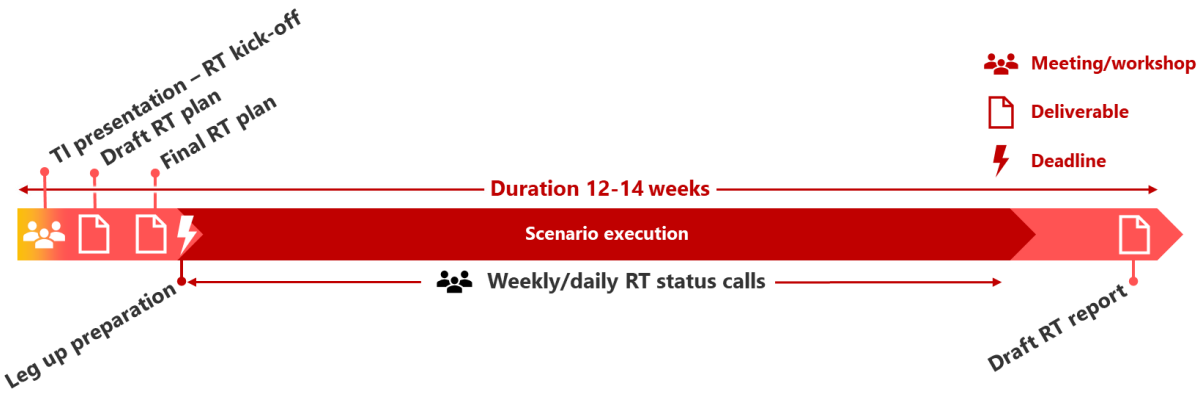

Figure 4 Timeline of the TIBER-BE Red Team phase

6.2 Red Team Test Plan

Using the Targeted Threat Intelligence report delivered by the TI provider, the RT provider will draft a Red Team plan detailing the approach the RT will take. In this plan, the RT provider is expected to further specify the TTPs it will use and deliver a detailed timeline for each scenario, including planned TTPs and a description of the leg ups required if these TTPs would be unsuccessful. The plan will be shared with the WT and TCT, allowing them to provide feedback and suggest improvements or clarifications to the plan where desired. The TIBER-BE Red Team test plan guidelines suggest each scenario is split up into four distinct phases (RECON – IN – THROUGH – OUT) to categorize the TTPs used by the RT in a convenient manner. Furthermore, it is requested that the Red Team also maps all TTPs it will use to the MITRE ATT&CK framework to get a clear and standardized overview of the proposed attack plan.

An important part of the RT test plan handles alternative approaches and required leg ups. The RT is expected to anticipate any issues during testing (detections, ineffective TTPs, etc.) by formulating alternatives to the chosen TTPs or potential leg ups that could be used to further the test. It is, of course, difficult to define specific leg ups in advance of testing, but the RT is requested to make some suggestions as to what leg ups could be considered in each stage of the scenario execution and

when to execute them at the latest. The WT is also encouraged to foresee some generic leg ups before the actual start of the RT phase. This is especially the case for leg ups that require some time to prepare, such as the provision of a lambda user account or a company laptop from where the RT can perform its testing.

6.2.1 Additional information delivered to the Red Team

The TIBER-BE process is designed to create realistic threat scenarios mimicking recent and possible future attacks. Real-world threat actors may have months to prepare an attack. They are also able to operate free from some of the constraints that TIBER-BE service providers must respect, such as the time and resources available – 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.

A similar constraint relates 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 common connecting infrastructure, the knowledge of the functioning of these systems may be limited for a RT provider, especially in comparison to those attackers with the capacity and time to study these extensively.

Therefore, the WT is free to provide additional information to ensure the RT provider has the right level of information to mimic advanced attacks. Thus, a TIBER-BE engagement reflects a 'grey box' testing approach, in contrast with the 'black box' approach. The RT provider receives support from the WT to compensate for the fewer possibilities it has compared to, for instance, advanced persistent threats (APT). Experience shows that the more relevant information an organisation gives to the RT provider, the more the participating organisation will gain from the test. Of course, there will be a balance to observe. The claim may never be made in hindsight that the test was manipulated, and a real attacker could not have the information. Therefore, it should be plausible, based on the WT's expert opinion, that the information given to the RT provider could have been obtained by an advanced attacker, given more time, different known techniques, etc. Whether this information is provided by the WT or delivered by a Third-Party TI provider, is up to the WT and must be documented as an information leg up.

Before finalising the RT test plan, a draft is to be submitted to the WT and TCT for review. In this review, the WT can identify approaches or TTPs that it considers to be ineffective and disclose this information to the Red Team. In general, disclosure of such information to the Red Team is not encouraged as it hinders the goal of a TIBER-BE engagement to uncover unknown gaps in the CI's security controls. However, when motivated properly and in consultation with the TCT, the TCT can agree to communicate such reservations about the RT Plan to the RT provider.

The Concerned Institution can also choose to wait in providing any additional information to the Red Team, until the Red Team phase is ongoing. This way, it is possible to gauge the ease by which an attacker could collect any relevant information by themselves. Information provided by the Concerned Institution can then be considered a leg up, helping the Red Team to progress through the test.

6.3 Test execution

6.3.1 Execution of the scenarios

Once the Red Team test plan is approved by the WT and the TCT, the execution of the scenarios can begin. In the RT test plan, the Red Team has detailed the specific TTP's that will be used as well as a timeline roughly setting out each scenario sub-phase (RECON-IN-THROUGH-OUT). However, as the scenarios and test plan were developed using a grey-box approach, the Red Team has no complete knowledge of what they will encounter throughout the test. Therefore, a more pragmatic approach is required when executing the different scenarios, allowing for small deviations from the test plan as the Red Team gains better insight into the infrastructure and security controls in place.

The objective of the Red Team is to capture the flags related to each of the scenarios. To achieve this objective, the Red Team must progress through the different sub-phases of each scenario. Of course, the actions undertaken by the RT are to be shared with and approved by the WT, especially the actions related to capturing the flags. The execution of each scenario should be performed in a stealthy way as to avoid detection by the Blue Team, consistent with the modus operandi of real threat actors. When detection events do occur, the White Team is encouraged to let the BT follow normal detection and response procedures of the CI without informing the defenders of the test. However, there are some cases where intervention by the White Team is justified:

- The Blue Team is considering an external escalation, such as reporting the observed actions to authorities or other third parties.
- Preventing business impact that would be caused by the BT normal response procedure.
- The Blue Team is under significant strain, compromising the team's ability to respond to other (real) attacks.

When it is deemed necessary to inform the Blue Team, care must be taken not to immediately disclose the nature of the test, the entire TIBER-BE test or all its scenarios. If possible, it is preferred to inform the BT only of the actions performed so far in the detected scenario (only partially disclose the test). This way, other testing activity can continue without the knowledge of the BT, keeping the Red Teaming nature of these TTPs.

In a TIBER-BE engagement, all subphases of a scenario (RECON-IN-THROUGH-OUT) should be executed, as to test the CI to the fullest extent. For this reason, provisions should be in place to aid the RT in case full scenario execution is hindered (e.g. by security controls, detection, time constraint, etc.). Normally, one or more leg ups are provided to the Red Team in such a situation. However, if it is deemed unlikely that the RT can continue without detection by the Blue Team, a purple teaming element can be considered. Both leg ups and purple teaming are explained in further detail below.

6.3.2 Red Team status updates

The Red Teaming phase is the most critical phase of a TIBER-BE engagement. Red Team testers are actively attacking the live production systems in their search for the set flags and relevant findings. This activity inherently comes with risks to the CI's business operations, balanced by the risk mitigating actions taken in the preparation phase. It is therefore essential that the WT and TCT are aware of the actions planned and performed by the RT, ensuring the test can be conducted in a controlled manner.

During the Red Team phase, the WT will be in close contact with the Red Team testers. A short daily meeting or call should be arranged for this purpose. On these daily update calls, the RT will inform the WT about any issues encountered as well as the activities planned for the next day. Additionally, a more continuous channel of communication could be set up, such as a secure instant messaging channel, to update the WT (and possibly the TCT) on the RT activities the moment they occur.

Besides the WT, the TCT should also be updated on a regular basis about the RT activities and any potential issues encountered. For this, a weekly update by the RT suffices. During this weekly call, the RT is expected to give an overview of the activities performed the past week, the findings made so far, any issues or blocking factors, and the activities planned for the coming week along with an updated project plan. A template slide deck for this meeting is provided by the TCT by means of guidance, the RT provider is free to decide how to present the information requested.

Participation of the TI provider is also encouraged for these weekly calls to support the Red Team and provide input. One specific example where TI input could be beneficial is during the reconnaissance activities performed by the RT. The passive nature of the reconnaissance activities performed in the TTI phase might result in a gap between the information provided by the TI provider and the information the RT needs to properly execute the prescribed scenarios. For this reason, the RT often performs a preliminary active reconnaissance to gain additional insights that could be useful

for the scenario execution. Any findings made through the Red Team's active reconnaissance activities could be shared with the TI provider who can in turn give advice on how the emulated threat actor would make use of such findings thus potentially influencing the planning or execution of the scenarios.

In case any critical issue is encountered during testing, an ad hoc meeting can be scheduled between the RT, WT and TCT to discuss and look for possible solutions together.

6.3.3 Leg ups

As stated above, the Red Team is subject to several limitations compared to the threat actors emulated when executing TIBER-BE RT scenarios. Due to these limitations, it is likely that the RT will face difficulties in successfully executing a scenario as drafted by the TI provider. The TIBER framework has taken this into account by enabling the activation of measures that would allow the RT to proceed with the scenario, known as "leg ups".

A leg up can be defined as an action through which the WT assists the RT in executing the scenario and capturing the related flags. Leg ups serve to maximize the value of a TIBER-BE engagement as they allow the RT to proceed in executing the scenario, possibly enabling the identification of findings in the latter stages of the test. The leg up that is provided strongly depends on the scenario and the level of access available to the RT. Leg ups can be categorised in several ways:

- **Time saving leg ups**: These leg ups are granted to expedite the progress of the RT. The RT is not necessarily blocked but would require significant time to proceed in the scenario execution. (e.g. Identifying suitable target machines on an internal network the RT has access to)
- **Information leg ups**: These leg ups provide the RT with information on how to proceed in the scenario. (e.g. Explaining why a payload used by the RT was blocked/detected, allowing the RT to make adaptations)
- **Access leg ups**: This is a leg up where the WT makes use of its access to the internal network to perform an action that would help the RT (e.g. as an accomplice opening a phishing email). The WT can also provide access for the RT, granting them a foothold in the internal network. (e.g. RT is provided with an account that has a specific access)

The RT is expected to anticipate any leg ups they could require during the scenario execution, identifying them in the RT test plan. Having the leg ups known in advance also enables the WT to adequately prepare for the leg up activation. This minimizes the risk of delays during testing, as the leg up can be prepared well before it is actually needed. Activation of a leg up should be done in consultation with the TCT.

6.3.4 Critical findings

When the Red Team uncovers a (chain of) finding(s) that is considered critical by the TCT, the TCT reserves the right to temporarily pause the test allowing the CI to remediate the vulnerability and mitigate the immediate risks arising from the finding. In such a case, the TCT acts in the NBB's responsibility to safeguard the stability of the financial system, mitigating any direct risks to the concerned institution and by extension the financial system. Once the appropriate mitigating actions have been performed, the test can resume. Ideally, the TIBER-BE test is continued in a covert manner as per requirement of the TIBER-BE methodology. It is clear, however, that disclosure of the test is more likely when a critical finding must be remediated immediately. In case the test needs to be disclosed to the BT, the stakeholders can jointly decide to continue the testing in a Purple Teaming setting, involving the BT in the remainder of the test. Purple teaming is further discussed below in section 6.3.6.

Any critical findings discovered during the test and the immediate actions taken to mitigate the risk must be clearly indicated in the final test summary report. After the TIBER-BE test is concluded,

further investigation by the Concerned institution will be required, verifying the causes and impact of the identified critical vulnerability. An 'assume breach' investigation is also recommended, investigating the possibility the vulnerability was already exploited by an undetected threat actor. The TCT will not be involved in these investigations. However, sharing and openness on topic could result in assistance from and to other members of the community.

6.3.5 Scenario X

As TIBER-BE scenarios aim to emulate known threat actors using their previously observed TTPs, it is likely that mature institutions have sufficient security controls in place preventing complete execution of a scenario, even with the use of leg ups. In such a case, the TIBER-BE engagement serves as a validation of the implemented security controls, adding to the CI's assurance that the institution is adequately protected against the emulated threat actors. However, to get the most value from a TIBER-BE engagement, mere validation of the existing security controls is not enough. Ideally, a TIBER-BE test also identifies points of improvement, where existing controls can be improved. To this end, the TIBER-BE has implemented the concept of a Scenario X, enabling a more pragmatic and opportunistic approach to testing.

A scenario X can take different forms and can be both part of the Red Teaming as the purple teaming phase. It allows the different participants of the TIBER-BE engagement to adopt a more pragmatic approach in identifying interesting avenues of attack and/or new targets that are not necessarily part of the threat intelligence-based scenarios. Some examples of a scenario X implementation are listed below:

- The CI wants to test a specific system that is not in scope of the TI-based scenarios;
- The CI wants to test some specific TTPs that are not part of the TI-based scenarios;
- The RT wants to leverage tools and TTPs that are not described in the TI-based scenarios
- During the test, the RT discovers interesting findings that could be leveraged but that are not in line with the TI-based scenarios.

6.3.6 Purple Teaming during the RT phase

Purple teaming is defined as testing activity whereby both RT and BT are aware the test is taking place. However, the exact implementation of a purple teaming approach can take a variety of shapes and forms. In this document, a short overview on the different ways of implementing purple teaming is given.

One of the defining elements of a purple teaming implementation is where it is situated in the overall testing timeline. In practice, purple teaming can be implemented as part of the active RT phase, as part of the closure phase or as a combination of both. In this section, purple teaming as part of the active RT phase is described.

During the Red Teaming phase, several occurrences can trigger a shift towards a purple teaming approach. In general, purple teaming becomes an option when no more possibility to continue testing without involving the BT can be envisioned for a scenario or for the entire test. When such a situation occurs, the White Team can make the decision, in consultation with the TCT, to disclose the test or the corresponding scenario(s) to the BT.

In most cases, purple teaming during the RT phase is implemented as a "catch-and-release" type of exercise. The BT is made aware that a test is taking place, but the details of the test, such as the scenarios and actions that will be performed by the RT are not shared. The BT will then communicate any detections of suspicious activity to the WT and if the detections concern TIBER-BE Red Team activity, no response should be performed by the BT. Of course, all detections of TIBER-BE Red Teaming activity should be included in the test summary report as to accurately illustrate the BT detection capabilities.

6.4 Red Team Report

When all testing activities are concluded, the RT provider drafts a Red Team report giving a detailed overview of the test. The RT provider is free to choose the report template that is used as long as the report contains following aspects:

- An executive summary describing the test and the most important findings
- A detailed timeline describing all the RT actions and relevant information including target systems and possible artifacts that remained on the CI network (this could be a separate document as well)
- Description of each of the scenarios detailing the TTPs used, any leg ups that were required and the results obtained.
- List of findings done by the RT, ranked by the provider according to severity, in the context of implemented security controls
- Provider recommendations for each finding

At the end of the RT phase, a draft version of this report is to be delivered to the WT. The final version of the report can be delivered during the closure phase of the engagement allowing the inclusion of any potential additional findings that are identified during the replay and purple teaming activities.

Given the sensitive information contained in the RT report, the report should only be shared with the Concerned Institution. The TCT is not expected to receive a copy of the report but will usually request to consult the report on CI premises for review and feedback before the final version.

7. Closure Phase

7.1 Overview

When the Red Team phase is concluded, the TIBER-BE engagement moves into its closure phase. During this phase, several workshops are held, and reports are expected from the different participants of the TIBER-BE engagement. The goal of the closure phase is to provide an overview of the entire TIBER-BE engagement and its related findings, draft a remediation plan and to give feedback to the performance of all parties involved in the engagement.

Relevant documentation:

- Red Team report (draft)
- TIBER-BE test summary report guidelines
- TIBER-BE 360° feedback template

Workshops held in the closure phase:

- Replay workshop
- Purple Teaming Workshop (optional and circumstantial)
- 360° Feedback Workshop

Output of this phase:

- Blue Team Report
- Red Team Report (final)
- Test Summary Report (containing remediation plan)
- TIBER-BE attestation

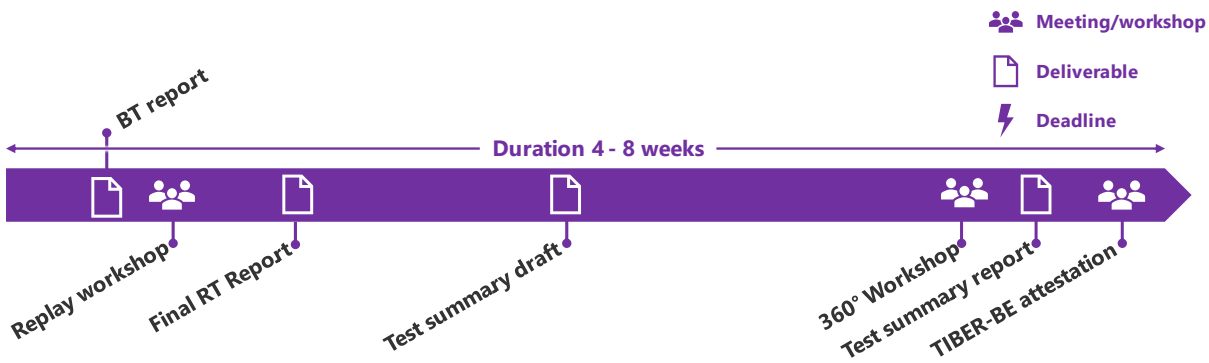

Figure 5 Timeline of the TIBER-BE closure phase

In what follows, each element of the closure phase will be discussed in further detail.

7.2 Blue Team Report

Once the active RT phase is finished, the test can be disclosed to the BT. The BT is briefed of the scope of the assessment and is provided with a high-level overview of the compromising actions performed by the RT. Using this information, the BT is expected to list any detection and response processes that were performed during the testing timeframe and that could be linked to the RT testing activity. This information is then combined in a BT report, that will serve as input for the next steps in the TIBER-BE closure phase. In general, the BT report will contain following information:

- **Detection and response events**: The actions performed by the RT could/should have triggered detections by the BT. As the BT was not aware that a test was ongoing, normal detection and response procedures should have been followed. The detections, mitigating actions and escalation events performed by the BT, must be included in the BT report.
- **Logging events**: Upon disclosure of the testing activities, the BT can examine the logs and verify if any suspicious RT activities were logged that did not (or not immediately) trigger a detection and response process. All logging events identified only after completion of the covert activities of a TIBER engagement should be documented as such and be clearly distinguishable from the events that were detected and responded to during these activities.
- **Timeline**: All detection and response events and logging events should be included in a detailed timeline. This timeline will be used further in the closure phase to align and match RT and BT actions. It is important to make a clear distinction between logging events not acted upon, and detection/response events by the BT. Reporting these events clearly in the timeline enables the analysis of any delays that might exist between logging, detection and response which could lead to additional learnings from the TIBER-BE engagement.

7.3 Replay & Purple Teaming Workshop

7.3.1 Replay workshop

One of the requirements of TIBER-BE is the organisation of a replay workshop. In the replay workshop, RT and BT come together to perform a walkthrough of the actions performed by both teams during the test. This workshop can therefore only be organised after the delivery of the BT report, as a detailed timeline from both RT and BT is required for an in-depth discussion on the assessment. The required participants for this workshop are the Red Team, the Blue Team and the White Team. Participation of the TCT in this workshop is not a requirement, but it is encouraged. If deemed useful by the WT, it is also possible to include the TI provider in this workshop to provide further insight in the scenarios they developed.

Typically, the replay workshop is comprised of two main parts. First, a “tabletop” walkthrough of the test is performed, comparing RT and BT timelines. RT and BT explain their actions in further detail

where required. The goal of this tabletop walkthrough is to identify areas where further investigation could be beneficial (e.g. RT actions that went undetected by the BT or BT detections that could be avoided by making small adjustments to the RT approach). The second part of the replay workshop is more hands-on. Where possible, the RT re-enacts (part of) some of the attacks performed during the Red Teaming phase and the BT investigates whether they can detect these attacks and respond accordingly. This can be an iterative process, where slight modifications are made to both RT and BT actions, maximising the learning value for both parties.

The duration of the replay workshop can vary, but it is recommended to reserve at least two sessions of half a day for it. Organizing a full day of replay workshop is not recommended as to avoid keeping the BT from their actual job of protecting the CI.

7.3.2 Purple Teaming during the closure phase

The replay workshop can be augmented with a Purple Teaming element or, an additional purple teaming workshop can be organised during the closure phase. Such a purple teaming workshop is encouraged under TIBER-BE. It allows the WT and the CI to go beyond the scope of the original assessment, exploring possible attack paths that could not be executed during the Red Team phase. This approach can be used, for example, in cases where the proposed Red Team attack path was deemed too risky to be performed in a covert manner. Purple teaming allows for the involvement of additional subject matter experts, reducing the risk of certain RT actions.

7.4 Test Summary Report

When both the Red Team and the Blue Team have finalised their reports, the White Team is expected to compile a Test Summary report. This report combines the RT and BT views on the test and provides a high-level overview of the course of the TIBER-BE engagement. As a guide to the WT, a Test Summary report Template will be made available by the TCT, containing all required elements of the test summary report.

- Executive summary
- Scope of the assessment
- Scenarios developed by TI provider
- High-level outcome and findings
- Recommendations made by the RT
- Attack summary
- Remediation plan

It should be clear that some elements of the test summary report can already be completed during the test preparation and execution phases. The WT is therefore encouraged to start with drafting the test summary report early in the engagement, reducing the report effort required in the closure phase.

The test summary report aims to give a complete overview of the TIBER-BE engagement and its outcomes. As such, the WT is expected to list all findings made during the test. However, given the sensitive nature of the information, it is advisable that only a high-level description of the findings is included in the test summary report. Especially as this document will serve as the basis for information sharing at the end of the TIBER-BE engagement. The test summary report is to be shared with the TCT who will review it and provide feedback where necessary. The CI will remain owner of the final document and has no obligation to distribute it to other parties. However, the CI is strongly encouraged to share the test summary report with the relevant supervising authorities at the end of the TIBER-BE engagement.

7.5 360° Feedback Workshop

In the 360° feedback workshop, CI, TCT, TI and RT provider come together to review the TIBER-BE engagement on a more meta level, giving feedback on the TIBER-BE process, the national

implementation guide, and on the performance of each participant involved in the engagement. As the TIBER-BE national implementation is of an evolving nature, such feedback workshops are paramount to improve the framework and the way in which providers, TCTs and CIs approach TIBER-BE engagements. The TCT will arrange and facilitate this workshop, moderating the discussion to allow every participant to share experiences and provide feedback.

In preparation of this workshop, the TCT will send out a 360° feedback questionnaire to each participant. The participants are expected to fill in this questionnaire and return it to the TCT before the workshop. The TCT will use the answers provided as input to moderate this discussion, but the filled-in questionnaires will not be shared with the other participants.

7.6 TIBER-BE attestation

When all TIBER-BE requirements[1] are met and the required reports have been delivered to the TCT, a TIBER-BE test attestation is delivered. This attestation is a document signed by all participants of the engagement[2] and declares that the assessment adhered to the TIBER-BE requirements. Therefore, the TIBER-BE attestation document is proof to other authorities that the CI has successfully completed a TIBER-BE assessment and can serve as the basis of mutual recognition of the engagement.

7.7 Result sharing

As mentioned in the beginning of this document, one of the core objectives of the TIBER-BE implementation is to improve the cyber resilience of the Belgian financial sector. In the first place, TIBER-BE aims to achieve this goal by enabling selected entities to identify any weak points by means of performing a TIBER-BE assessment. Therefore, the main purpose of a TIBER-BE engagement is to indicate where potential improvements to the tested entity's cyber posture might be necessary. Nevertheless, under the TIBER-BE national implementation, the tested entity is required to deliver a *Test summary Report* to the TCT, describing the assessment, its findings, and a proposed remediation plan. It is also strongly encouraged this Test Summary report is shared by the CI with the relevant supervising/overseeing authorities enabling the follow-up of the remediation plan as well as the identification of sector-wide points of attention.

Another manner through which the TIBER-BE national implementation aims to contribute to cyber resilience of the Belgian financial sector is by ensuring that the lessons learnt from a TIBER-BE engagement are shared among peers such that the broader financial sector can benefit from them. To this end, the TIBER-BE community was established, bringing together all financial institutions in scope of the TIBER-BE national implementation. All members of the TIBER-BE community assemble on a biannual basis during the TIBER-BE National Implementation Committee (NIC). On the NIC, a variety of information can be shared between the members of the TIBER-BE community, such as an overview of the current cyber threat landscape, lessons learnt from previous TIBER-BE engagements, specific topics requested by the TIBER-BE community and other items relevant to the TIBER-BE national implementation and the cyber resilience of the Belgian financial sector.

As such, each CI is encouraged to present their experience to the broader TIBER-BE community upon finalising a TIBER-BE engagement. Topics to present can range from lessons learned to improve the implementation of specific security controls, to best practices when coordinating a TIBER-BE engagement. As the TIBER-BE NIC is a trusted group, all information shared during this meeting is to be considered as confidential, and information will only be shared with the TIBER-BE community with consent of the concerned institution.

[1] A list of TIBER-BE minimum requirements is provided in Annex II

[2] The TCT (represented by the TIBER-BE programme manager), the CI (represented by the sponsoring board member), the TI provider, the RT provider and any other relevant authorities that were involved in the engagement.

8. Annex

8.1 ANNEX I: overview of deliverables and meetings in the TIBER-BE process

Name	Type	Phase	TCT	WT	TI	RT	BT	SUP/OVS
Pre-Launch meeting	Meeting	Preparation	R, A	I				
Launch meeting	Meeting	Preparation	C	R, A				
Project planning	Deliverable	Preparation	S, I	R, A				
TI Provider procurement - shortlist	Deliverable	Preparation	S, I	R, A				
RT provider procurement - shortlist	Deliverable	Preparation	S, I	R, A				
Scoping document	Deliverable	Preparation	S, I	R, A				C
Risk management document	Deliverable	Preparation	S, I	R, A				
Scope attestation	Deliverable	Preparation	I	R, A				
Scope presentation	Meeting	Preparation	S, I	R, A	I	I*		
TTI Kickoff	Meeting	Threat Intel		R, A	C, I			
TTI Midpoint Workshop	Meeting	Threat Intel	C, I	C, I	R, A	C*, I*		
TTI Report (Target & threat intel + scenarios)	Deliverable	Threat Intel	I	I	R, A	I		
TTI Report Presentation	Meeting	Threat Intel	I	I	R, A	I		
RT Test Plan	Deliverable	Red Teaming	S, I	C, I	I	R, A		
Leg up preparation	Deliverable	Red Teaming	S	R, A	S	C		
RT execution Kickoff	Meeting	Red Teaming	I	S		R, A		
RT regular update meetings	Meeting	Red Teaming	S, I	C, I	S, I	R, A		
Purple Teaming (Optional)	Meeting	Red Teaming	I	R, A	S	S, C	S, C	
BT Report (incl. BT timeline)	Deliverable	Closure	I	S, I		I	R, A	
Replay workshop	Meeting	Closure	I	R, A	S	S, C	S, C	
Purple Teaming (Optional)	Meeting	Closure	I	R, A	S	S, C	S, C	
RT Report	Deliverable	Closure		I		R, A		
360° questionnaire	Deliverable	Closure	R, A	R	R	R	R	
360° workshop	Meeting	Closure	R, A	C, I	C, I	C, I	C, I	
Test summary report	Deliverable	Closure	S, I	R, A			C	(I)
Final meeting	Meeting	Closure	S	R, A				
Test attestation	Deliverable	Closure	R, A	S	S	S		I
R = Responsible, A = Accountable, S = Support, C = Consulted, I = Informed, * = if already onboarded								

8.2 ANNEX II: Minimum requirements for obtaining TIBER-BE attestation

a. Minimum requirements for the White team

- Establishing a White Team (WT) responsible for Concerned Institution's own management and organisation of the TIBER-BE test process, including for producing and maintaining a project plan.
- Procuring independent external provider(s) responsible for the targeted threat intelligence (TI provider) and the red team test (RT provider).
- Ensuring that the TI/RT provider(s) meet the minimum requirements set out in the TIBER-EU Services Procurement Guidelines.
- Developing the scope of the test which includes Concerned Institution's critical functions (CFs), including the people, processes and technology and databases that support the delivery of the CFs.
- Arranging the scoping meeting, where the proposed scope of the test is discussed and finalised, and the targets and objectives of the test are agreed upon.
- Documenting the scope in the TIBER-BE Scope Specification Template which was signed off by a member of Concerned Institution's Executive Board.
- Arranging the launch meeting with all relevant stakeholders, i.e. WT, TCT, TI/RT providers, where the overall project plan was discussed and agreed upon.
- Conducting a risk assessment and put in place the necessary risk management controls, processes and procedures to facilitate a controlled test.
- Providing information in advance to the TI provider by using the TIBER-BE Guidance for Targeted Threat Intelligence Template.
- Providing feedback to the TI provider during the process of developing the Targeted Threat Intelligence report and the threat scenarios.
- Facilitating the Threat Scenario review process.
- Facilitating the handover session between the TI and RT providers.
- Providing feedback to the RT provider during the process of developing attack scenarios and Red Team Test Plan.
- Securing the legal soundness of the test, i.e. that the test will not contravene any national or European laws or regulations.
- Allowing test to be executed on live production systems.
- Continuously being in contact with the RT provider during the execution of the test, including approving progress, and providing "legs-up" if needed.
- Securing that only the WT and TCT are informed about the test, its details and the timings – all other staff members (outside the White Team) remained unaware during the execution of the test.
- Providing feedback to the RT provider during the process of drafting the Red Team Test Report when the test was finalised.
- Facilitating replay workshops between the Red Team and relevant members of the Blue Team.
- Producing a Blue Team Report, where Concerned Institution's own IT-security team mapped its actions alongside the Red Team's actions.
- Participating in the 360-feedback meeting.
- Producing a Remediation Plan.
- Producing a Test Summary.

b. Minimum requirements for the Threat Intelligence provider

- Meeting minimum requirements for TI providers set out in the TIBER-EU Services Procurement Guidelines.
- Participating in the launch meeting.
- Using the Generic Threat Landscape Report as a basis for drawing the targeted threat landscape for Concerned Institution and adding to the threat landscape where relevant.

- Producing a Targeted Threat Intelligence Report for Concerned Institution following the requirements in the contract with Concerned Institution, such that it at a minimum meets the requirements in the TIBER-BE Guide.
- Securing the legal soundness of the test, i.e. that collection of threat intelligence will not contravene any national or European laws or regulations.
- Arranging the handover session with the RT provider.
- Continuing to be engaged during the testing phase and provided additional up-to-date, credible threat intelligence to the RT provider, where needed.
- Participating and providing input to the post-test replay, if relevant.
- Participating/contributing in the 360-feedback, Remediation Plan and Test Summary

c. Minimum Requirements for the Red Team provider

- Meeting minimum requirements for RT providers set out in the TIBER-EU Services Procurement Guidelines.
- [Participating in the launch meeting.]
- Participating in the handover session with the TI provider.
- Developing multiple attack scenarios, based on the Targeted Threat Intelligence Report.
- Producing the Red Team Test Plan.
- Securing the legal soundness of the test, i.e. that the execution of the test will not contravene any national or European laws or regulations.
- Executing the attack based on the scenarios (with some flexibility) in the Red Team Test Plan and going through each of the phases of the kill chain methodology.
- Keeping the WT and TCT informed about progress during the test, “capture the flag” moments, the possible need for leg-ups, etc.
- Taking a stage-by-stage approach and consults the WT and TCT at all critical points to ensure a controlled test. The total time/effort spent on testing was in line with the applicable framework(s).
- Producing a Red Team Test Report for Concerned Institution following the requirements in the contract with Concerned Institution, such that it at a minimum met the requirements in the TIBER-BE Guide.
- Participating in replay workshops between the Red Team and relevant members of the Blue Team.
- Participating/contributing in the 360-feedback, Remediation Plan and Test Summary

9. References

[1] European Central Bank (2018), *TIBER-EU Framework,*

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

[2] European Central Bank (2018), *TIBER-EU White Team Guidance*,

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

[3] Bank Of England, Prudential regulation Authority (2021), *CBEST Threat Intelligence-Led Assessments*, Available from https://www.bankofengland.co.uk/-/media/boe/files/financial-stability/financial-sector-continuity/cbest-implementation-guide

[4] European Commission (2020), *Proposal for a regulation of the European Parliament and of the Council on digital operational resilience for the financial sector*,

Available from https://data.consilium.europa.eu/doc/document/ST-11051-2020-INIT/en/pdf

[5] European Central Bank (2018), *TIBER-EU Services Procurement Guidelines*, Available from https://www.ecb.europa.eu/pub/pdf/other/ecb.1808tiber_eu_framework.en.pdf

[6] European Central Bank (2020), *TIBER-EU Guidance for the Target Threat Intelligence Report*, Available from https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/shared/pdf/Final_TIBER-EU_Guidance_for_Target_Threat_Intelligence_July_2020.pdf

[7] European Central Bank (2020), *TIBER-EU Guidance for the Red Team Test Plan*,

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

[8] European Central Bank (2020), *TIBER-EU Guidance for the Red Team Test Report*,

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