Threat Intelligence Based Ethical Red Teaming

TIBER-BE framework
National Implementation Guide

Version 1.2

June 2020

Traffic Light Protocol: white

Contents

1. Introduction 3

1.1 Background 3
1.2 Purpose of this guide 4
1.3 Responsibilities and liability 4
1.4 Legal disclaimer and copyright notice 4

2. TIBER-BE overview 5

2.1 Introduction 5
2.2 Stakeholders 5
2.3 Process overview 5
2.4 TIBER-BE Team 5
2.5 Managing the risks involved during the test 7

3. Generic Threat Intelligence 8

3.1 Overview 8
3.2 External Intelligence Specialists 8
3.3 Threat Intelligence Sharing Platform 8

4. Preparation Phase 9

4.1 Overview 9
4.2 Pre-launch and Procurement 9
4.3 Launch 10
4.4 Scoping 10
4.5 Risk assessment 10
4.6 Scoping meeting 10
4.7 Scope explained to TI provider / RT provider 11

5. Test Phase 12

5.1 Overview 12
5.2 Target Intelligence delivered by the RT provider / TI provider 12
5.3 Test Plan 12
5.4 Scenarios 13
5.5 Additional information delivered by the Concerned Institution 13
5.6 Test 14

6. Closure Phase 15

6.1 Overview 15
6.2 Closure phase 15
6.3 RT Report and BT / RT Replay 15
6.4 360° feedback 16
6.5 Remediation plan, TIBER-BE TEST Summary, and sharing of results 16
6.6 Supervision 16

1. Introduction

1.1 Background

Belgian Critical Market Infrastructures and Core Financial Institutions (Concerned Institutions) must remain resilient to cyber-attacks that have a systemic impact. To help achieve this goal, the National Bank of Belgium (NBB) decided to adopt the TIBER-EU Framework (May 2018) to lead the implementation of a framework for Threat Intelligence-based Ethical Red teaming in Belgium: the TIBER-BE framework. The implementation of this framework involves a joint effort by market participants, whereby the NBB acts in execution of its task to contribute to the stability of the financial system. Articles 12, § 1 and 36/33, § 1 of the Law of 22 February 1998 establishing the organic statute of the National Bank of Belgium stipulate that the NBB shall be 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. Article 13 of the Law of 22 February 1998 allows the NBB to use the TIBER-BE framework as a tool to reach these objectives.

Within the TIBER-BE framework, the Concerned Institutions hire external cyber security providers to conduct controlled simulated attacks on their critical live production systems.

TIBER tests mimic potential attacks by real high level threat groups (organised crime groups / state proxies / nation-state attackers) and test whether the prevention, detection, response, recovery and decoy capabilitiesare effective (capability assessment), thus supplementing the current periodic information security audits (process assessments) performed by e.g. supervisors and overseers and the current penetration tests and vulnerability scans. Test scenarios will draw on current commercially obtained threat intelligence that will, where possible, be enriched and reviewed together with External Intelligence specialists. This testing method aims to determine, and importantly serves to improve the capabilities of targeted institutions. The TIBER-BE framework should improve their cyber resilience and ultimately, the cyber resilience and stability of the financial system as a whole. TIBER-BE testing will be a recurrent exercise.

A TIBER 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, without the foreknowledge of the organisation’s defending Blue Team (“BT”). The actual test consists of time-boxed phases (recon, in, through, out). As a consequence, existing controls, prevention measures, decoy and security detection and response capabilities against advanced attacks can be tested throughout all the phases of the attack. It also helps identify weaknesses, errors or other security issues in a controlled manner.

The test phase is followed by a replay and purple teaming between the Red Team (“RT”) and the Blue Team to identify gaps, address findings and improve the overall capabilities of the Concerned Institution. During the test, a White Team (“WT”) consisting of only the smallest number necessary of the Concerned Institution’s security and business experts will monitor the test and intervene when needed, e.g. when the test seems to lead to critical impact (during a test, business impact is allowed to a level agreed on beforehand, critical impact is not). The WT will be in close contact with the NBB’s TIBER-BE Team (“TBT”), who convoy the TIBER-BE test process.

Collaboration, evidence and improvement lie at the heart of TIBER. What differentiates TIBER from other security tests is its intelligence-led, holistic and live systems testing approach. This means that Concerned Institutions can improve their resilience based on proven relevant weaknesses rather than on perceived / possible weaknesses. This means that by using TIBER, a higher return on security investments can be obtained than by solely working with a compliance-driven risk framework and defending against perceived risks. In addition, the central role of the TBT enables comparison and the distillation of best practices.

1.2 Purpose of this guide

This guide has been developed by the TBT of 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 test.
This document is a guide rather than a detailed prescriptive method. It should therefore be consulted alongside other relevant TIBER-BE and TIBER-EU materials which will be provided by the TBT to TIBER-BE participants. This guide only details the TIBER-BE test process. The TBT is available to answer any questions that Concerned Institutions or external cybersecurity service providers might have on the TIBER-BE.

1.3 Responsibilities and liability

Each participant in a TIBER-test is exclusively responsible and liable for the execution of the tasks attributed to it by this framework, including compliance with applicable laws and regulations. It is the responsibility of each participant to conduct a review of existing laws and regulations to ensure that the execution of the tasks attributed to it does not contravene any such law or regulation and to take appropriate risk management measures (e.g. make relevant contractual arrangements) to enforce compliance.

Unless explicitly agreed otherwise, each participant bears its own costs and expenses for participating in a TIBER-test.

1.4 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.

2. TIBER-BE overview

2.1 Introduction

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

2.2 Stakeholders

The direct stakeholders involved in a TIBER-BE test are:

- the Critical Market Infrastructures and Core Financial Institutions ("Concerned Institutions"), in which only the White Team ("WT"), led by the White Team Lead ("WTL"), knows about the test;
- the Blue Team ("BT") which comprises all staff at the Concerned Institution who are not part of the WT;
- the TIBER-BE Team ("TBT") of the NBB;
- the Red Team provider ("RT provider") & the Threat Intelligence Provider ("TI provider").

In case of multi-jurisdictional exercises, the Concerned Institution together with the TBT agree on the authorities to be involved in the test depending on the coverage and location of the critical economic functions (CEFs).

If some countries are not in the scope of the test, the national TIBER authority from such country may request a separate test, where relevant.

2.3 Process overview

The TIBER-BE test process consists of four phases:

1. The **Generic Threat Intelligence** describes the role of the threat actors (including their TTPs and Modi Operandi or MOs) and the expected threat actor motivations. This document will where possible be enriched and reviewed together with external intelligence specialists.
2. During the **Preparation Phase,** the TIBER-BE test is formally launched, the WT is established, the scope is determined. A RT provider and a TI provider are procured.
3. During the **Test Phase,** the TI provider enriches target intelligence, and the RT provider prepares (format test plan) and executes an intelligence-led red teaming test against a specified target (systems and services that underpin one or more critical functions).
4. During the **Closure Phase,** a replay and a purple teaming exercise of the executed scenarios take place between the BT and the RT provider and eventually a Remediation Plan is finalised. The process is reviewed and prevention, detection, response, recovery and decoy capabilities are assessed. Findings are shared with peers if the benefit is greater than the risk.The Concerned Institutions inform their respective supervisor or overseer about the TIBER-BE test in their regular meetings.

2.4 TIBER-BE Team

2.4.1 TIBER-BE Team ("TBT")

The TBT consists of the TIBER-BE Program Manager ("TPM") and Test Managers ("TTM"). The role of the TBT is to make sure Concerned Institutions undergo tests in a uniform and controlled manner. During all phases of the TIBER-BE process, the WT closely cooperates with the TBT. The TBT 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 test for the participating Concerned Institution or third parties. The TBT has a close relationship with the WT but is not formally part of the WT. The TBT has a right to escalate (major) deviations from the TIBER 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.

The TTM will:

- align closely with the WTL to make sure the test follows the agreed procedure and meets the right quality level;
- make sure the individual tests fit the function of the Concerned Institutions, the threat actor intelligence and high level scenarios provided;
- assess the intelligence level of the public and private sector providers, and the level of the work of the RT provider and possibly the TI provider during the test;
- facilitate sharing and learning among participants in TIBER.

The TPM will:

- develop international cooperation with other TIBER-BE-like programs for testing;
- conduct R&D regarding intelligence, testing and talent development;
- continuously develop the TIBER-BE framework based on experiences during the tests;
- cooperate with the TIBER-EU Knowledge Centre.

2.4.2 Responsibilities of the TBT and WTL

The responsibility for the overall planning lies with the Concerned Institutions. The WTL in the Concerned Institutions coordinates all activities, including engagement with the service provider(s). Service provider(s) produce a planning for their services and inform the Concerned Institution so they can be factored into the overall TIBER-BE test project planning. Significant deviations in the original planning will be discussed with the TBT. The TBT has direct access to the service providers when needed.

The TBT agrees on the scope and the scenarios and ensures that the test is executed according to plan and is up to the standards of a TIBER-BE test. There has to be close cooperation between the TBT and the WTL and individual roles and responsibilities should be respected. When crucial decisions need to be made (e.g. deviations during the test from the scope agreed on) or unclarities or diverging opinions emerge, the TPM will be involved.

The TBT may remove the TIBER-BE label in all situations which compromise the performance, the quality or the secrecy of the test, 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 framework;
- 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 involved parties do not sufficiently collaborate with each other;
- etc.

The TBT will take its decision in consultation with the WT, unless the circumstances do not, in the opinion of the TBT, allow for this. The TBT 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 test. 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 tests.

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

2.5 Managing the risks involved during the test

TIBER-BE tests are associated with inherent elements of risk for all parties, due to the criticality of the target systems, the people and the processes involved in the tests.
Prior to conducting the test, the WT conducts a risk assessment and then puts in place all the necessary risk management controls, processes and procedures to facilitate a controlled test.

Throughout the end-to-end test process, in all documentation and communication between stakeholders a code name is used to conceal the identity of the institution being tested.

The Concerned Institutions make sure that when hiring external service provider(s) (whether a RT provider or a TI provider), there is mutual agreement on at least the following aspects: the scope of the test, boundaries, timing and availability of the providers, contracts, actions to be taken and liability (including insurance where applicable). In addition, close involvement of the TBT in each TIBER-BE test ensures that the test proceeds according to the agreed test scope, scenario, planning and process as described in the cooperatively developed framework documents.

Risks are also reduced by advanced planning, informing only a very select group of people in higher management of the test and the scope of the test, and by clearly defining the scope and predefined escalation procedures. Importantly, the Concerned Institutions remain in control of and remain responsible for the red teaming test. At any time, the WT can order a temporary halt if concerns are raised over damage (or potential damage) to a system. Trusted contacts within the WT positioned at the top of the security incident escalation chain help prevent miscommunication and avoid knowledge about the TIBER-BE test being leaked.

The testing should be flexible enough to mimic the (seen, current and potential future) actions of a real attacker *and* should be performed in a planned and controlled manner in order to (amongst other things) ensure uniform testing, protect those involved (e.g. indemnifications) and prevent damage. Both elements are essential in order to make sure the Concerned Institutions and its peers can learn and evolve, not only using their own but all relevant results and findings.

The following actions are examples of activities that are not allowed during the test:

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

Intentional interception or recording of communication in which the RT provider does not participate, should only take place in accordance with applicable legislation. Personal data should only be collected and processed when absolutely necessary, and in accordance with applicable legislation.

3. Generic Threat Intelligence

3.1 Overview

Generic Threat Intelligence (GTI) is provided by the NBB. During the Test Phase (chapter 5) the participants support the RT provider in connecting this generic TI to the scoping and the target intelligence.

The GTI consists of:

- threat actor intelligence (including motivation and modus operandi) on the most advanced actors relevant for the Belgian Concerned Institutions;
- additional information regarding the position of the Concerned Institution within the financial system and its corresponding critical functions that may be of interest to advanced attackers (threat actor aims);
- GTI serves as input for the Preparation Phase (specifically it provides input for the launch meeting, the scoping document and the Targeted Threat Report).

3.2 External Intelligence Specialists

External Intelligence Specialists will, where possible, validate and enrich the threat intelligence provided and the high level scenarios.

3.3 Threat Intelligence Sharing Platform

The GTI has been developed by a specialised external service provider (Top-down approach).
The Concerned Institutions and the External Intelligence Specialists are expected to exchange threat intelligence (Bottom-up) via a dedicated sharing platform.
The combination of the Top-down and Bottom-up approaches aims to deliver an up to date, specific and relevant GTI.

4. Preparation Phase

4.1 Overview

During the TIBER-BE Preparation Phase, the project is formally launched and the TBT starts engaging with the Concerned Institution. The scope is established and the Concerned Institution procures the service provider(s). The duration of this phase of work is approximately four to six weeks, not including the duration of the procurement process.

Relevant documents:

- TIBER-EU White Team Guidance;
- TIBER-EU Services Procurement Guidelines;
- Scope Specification and attestation Templates;
- Risk Management Template;
- Generic Threat intelligence document.

Outputs of this activity are:

- Establishment of the Concerned Institution's White Team and identification of all stakeholders by the Concerned Institutions for delivery to the TBT;
- List of the procured service providers by the Concerned Institutions for delivery to the TBT;
- Compliance analysis of the procured service providers to the TIBER-EU Services Procurement Guidelines produced by the Concerned Institutions for delivery to the TBT;
- Scope Specifications produced by the Concerned Institutions for delivery to the TBT and service providers;
- Scope attestation signed by a senior executive;
- Risk management documentation produced by the Concerned Institutions for delivery to the TBT and service provider(s);
- Project Planning produced by the Concerned Institutions for delivery to the TBT and service provider(s).

4.2 Pre-launch and Procurement

The pre-launch meeting marks the start of the planned and agreed-on TIBER-BE process. The TBT asks the Concerned Institution to identify the relevant stakeholders and to establish a WT. This comprises a select number of senior individuals who are experts and/or are positioned at the top of the security incident escalation chain. The WTL will make sure that they are aware of the TIBER-BE red teaming test, the need for secrecy and the process the team should go through in case the BT detects and escalates a TIBER-BE-related incident. The pre-launch meeting will be held with the WTL and additional WT members as the lead sees fit. During the pre-launch meeting, the TBT briefs the Concerned Institution on requirements for:

- the TIBER-BE process and documentation;
- stakeholder roles and responsibilities;
- contractual considerations;
- project planning.

As regards contractual considerations, smooth delivery of a TIBER-BE test requires that the process is transparent and that appropriate information and documentation flows freely between the relevant parties. To facilitate the free flow of information, participating parties will be subject to appropriate non-disclosure obligations.

After the pre-launch meeting, the Concerned Institution starts its procurement process and selects a RT Provider and a TI Provider to perform the test. Importantly, the Concerned Institution offers a

shortlist of potential providers to the TBT which will deliver a recommendation regarding the providers. However, the Concerned Institution remains fully responsibility for the choice of the providers

During Procurement the Concerned Institution:

- procures and takes onboard a RT provider and a TI provider based on TIBER-EU Services Procurement Guidelines;
- ensures that it has incorporated the NDA clauses into its service provider contracts;
- confirms and agrees the scope with the TBT and completes the Scope Specification;
- completes the Project Plan.

4.3 Launch

Since cooperation is key for a successful TIBER-BE test, the launch meeting is a physical meeting, which involves all the relevant stakeholders. During this meeting, all parties discuss the test process and their expectations. They can also discuss a draft TIBER-BE Project Planning.

4.4 Scoping

During the launch, the TBT provides the Concerned Institution with a Scope Specification Template . The Concerned Institution then starts working on a draft version of the Scope Specification. The TBT is available during the scoping process to clarify the requirements and is available to give feedback. Within the TIBER-BE framework, Critical Functions ("CFs") 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 system, it is a 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 technological systems. These critical technological systems, processes, and the people surrounding them, are the focus of TIBER-BE threat intelligence and red teaming. Flags are placed on the critical systems in the scope 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 TBT, who must approve them. The Concerned Institution is allowed to involve the RT provider and TI provider in the scoping process.

4.5 Risk assessment

Prior to conducting the test, the WT conducts and documents a risk assessment to ensure all the necessary risk management controls, processes and procedures to facilitate a controlled test are in place. This includes but is not limited to:

- in-scope systems prior to any testing should be part of the preparations to ensure that backup and restoration capabilities are in place and hev been tested ;
- protecting the confidentiality of the test via the use of Non Disclosure Agreements ;
- for the physical penetration a «get out of jail » letter

4.6 Scoping meeting

The final scope document is agreed on by the TBT during a workshop organised by the Concerned Institution. Importantly, the scoping will need to be agreed on at senior management/board level of the Concerned Institution (attestation).

4.7 Scope explained to TI provider / RT provider

For a test to be successful, it is important that the service providers understand the business of the Concerned Institution. Therefore, after the scoping and in case the service providers were not already involved during the scoping, a meeting is planned with the provider(s) in which the CFs and systems underpinning them (compromising these is the test objective) are explained. If the Concerned Institution feels that further interaction regarding the functioning of its business is necessary to arrive at realistic scenarios, this is very much encouraged.

5. Test Phase

5.1 Overview

During the Test Phase, target intelligence is performed on the Concerned Institution, the detailed test scenarios are built and the red team test is executed. These scenarios are built by the RT provider in the Test Plan. If the Concerned Institution outsources some critical functions to a third party, this service provider should be included in the test.
If critical findings relating to the Concerned Institution are discovered, the WT will be immediately informed and will decide on the next steps (e.g. putting the test on hold to fix the vulnerability,…). If critical findings relating to vulnerabilities relevant to other institutions are found, these are shared.

Relevant documentation:

- Test Plan Template;
- Generic Threat intelligence document.

Output of this phase:

- Targeted Threat Intelligence Report
- RT Test Plan;
- RT Test Report

5.2 Target Intelligence delivered by the TI provider

In this phase, the TI provider executes an initial furtive broad, intelligence-based targeting exercise of the kind typically undertaken by threat actors as they prepare for their attack. Active reconnaissance activities on the Concerned Institution are not part of the Targeted Threat Intelligence phase. The objective is to draw a picture of the Concerned Institution as a target from the attacker's perspective. The use of various methods (including OSINT[1], TECHINT[2], HUMINT[3] and intelligence-based initial targeting) is encouraged.
The TI provider holds a handover session with the RT provider, providing the basis for the threat scenarios.

The output of the Target Intelligence identifies, on a Critical Function-focused, system-by-system basis, the people, processes and infrastructure of the Concerned Institution. This includes information that is intentionally published by the institution or about the institution and internal information that has been deliberately or unintentionally leaked. This could include customer data, confidential material or other information that could prove to be a useful resource for an attacker.
The Targeted Threat Intelligence report delivered by the TI provider contributes to the development of the test scenarios by defining their narratives, likelihood, impacted Critical Function-supporting systems, corresponding flags, involved threat actors, their TTPs etc.….

5.3 RT Test Plan

In the RT Test Plan, the RT provider puts together attack scenarios for the RT Test which:

- Are based on the ones produced in the Targeted Threat Intelligence report
- map onto one or more Critical Function-supporting systems;
- combine the Threat actor intelligence and Target Intelligence and aligns these into credible and actionable scenarios;
- ;

1 Open Source Intelligence.
2 Technical Intelligence.
3 Human Intelligence.

- provides creative elements of TTPs that deviate from the original scenario if the entity anticipates changing circumstances or in case the first option does not work;
- would, if occurring in real life, have a destabilising effect on the financial stability;
- also provide some elements which test the response of the Concerned Institution, including evidence on whether the compromise action would be immediately detected or could have a fair chance of succeeding.

5.4 Scenarios

Scenarios should be built based on the Generic Threat intelligence document, the scoping and targeting information of the previous sections.

The scenarios are written from the attacker's point of view. The RT provider indicates various creative options in each of the attack phases based on various TTPs used by advanced attackers, to anticipate changing circumstances or in case the first option does not work. The scenario writing is a creative process. The TTPs do not only mimic those seen in the past, but combine techniques of the various relevant threat actors. The RT provider is allowed to adapt the original scenario if the maturity and the security posture of the Concerned Institution require it and in order to make the test as relevant as possible for the Concerned Institution (e.g. testing additional attack vectors like mobile, IoT,…).

In order to increase the relevance of the TIBER-BE tests, it is recommended to include physical red teaming in the scope of the test (e.g. planting a device at the entity), provided all necessary precautions and risk management measures are taken.

In addition to these scenarios, a scenario X is prepared. Scenario X is the scenario in which the RT provider is stretched to its absolute limits. This scenario enables a forward-looking perspective to the attacks. The TBT can function as a discussion partner or direct one to the relevant Concerned Institution for more information when needed. It could be beneficial to start the scenario X when the RT provider has already infiltrated the network, since this would provide interesting leads.

5.5 Additional information delivered by the Concerned Institution

The Concerned Institution can deliver additional information for the RT provider on the scenarios chosen, including on people, processes and systems targeted in the scenario. It is up to the Concerned Institution to decide on the level of detail of this information.

The TIBER process is designed to create realistic threat scenarios mimicking 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 observe, 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.

It is up to the Concerned Institution to set up contractual agreements with the RT provider regarding e.g. the inviolability of their employees' privacy. It is, however, important to note that privacy-related information is left out from test reports under all circumstances.

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 with a RT provider may be limited in comparison to those attackers with the capacity and time to study these extensively.
Therefore, it depends on the Concerned Institution how much information it is willing to give to make sure the RT provider is on the right level of knowledge to mimic advanced attacks. Thus, TIBER reflects a 'grey box' testing approach, in contrast with the 'black box' approach. The RT provider

receives support from the Concerned Institution itself in order to balance out the smaller amount of possibilities it has compared to high end attack groups. 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 evident 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 Concerned Institution or delivered by a Third Party TI provider, is up to the Concerned Institution.

The Test Plan also provides a planning for the execution of the test. The timespan for actual testing should be between ten and twelve weeks. Please note that for this reason there can be a difference between full time test weeks (for example six) and actual test weeks in the planning (ten to twelve), in order for the RT provider to be able to work in a stealthy manner.

5.6 Test

The RT provider now moves into execution of the RT Test, during which the RT provider performs a stealthy intelligence-led red teaming exercise against the target systems. The RT Test takes approximately twelve weeks, or longer if felt necessary. The scenarios are not a prescriptive runbook which must be followed precisely during the test. If obstacles occur, the RT provider should show its creativity (as advanced attackers would) to develop alternative ways to reach the test objective. This of course is always done in close contact with the WT and the TBT. All actions of the RT provider are logged for replay with the BT, evidence for the Red Team Report and future reference.

The test objectives (compromise actions) are the ‘flags’ that the RT provider must attempt to capture during the test as it progresses through the scenarios. Of course all captures are performed in close cooperation with the WT and the overall aim is to improve the BT capabilities. The scenario is to be played out from beginning to end. The RT provider may need some help to overcome barriers, it may be discovered, etc. but the scenario must continue to make full use of the TIBER-BE exercise within the given timeframe and test all phases of the test (recon, in, through, out).

RT providers are constrained by the time and resources available as well as by moral, ethical and legal boundaries. Therefore, the RT providers may require occasional steers from the WT to help them progress. Should this happen, these steers are duly logged. This ensures that maximum benefit is derived by all stakeholders from a time-limited test.

At all times the RT provider liaises closely with the WT and with the TBT. The TBT is updated at least once a week by the RT provider and WT on the progress. Physical meetings between the WT, TBT and RT provider during this phase are strongly encouraged since the discussions add significantly to the quality of the test.

6. Closure Phase

6.1 Overview

The duration of the close-down activities in this final phase of work is approximately four weeks.

6.2 Closure Phase

The entity's senior management/board and the TI/RT providers sign an attestation to validate the true and fair conduct of the TIBER-EU test and to enable recognition by other relevant authorities.

The output of this activity is a version of the RT Test Report produced by the RT provider for delivery to the Concerned Institution. The draft report must be issued within two weeks of test completion. The BT is informed of the test and uses the RT Test Report to deliver its own BT report. In the BT report, the BT maps its actions alongside the RT actions.

Relevant documentation:

- RT Test Report Template;
- TIBER-BE Test Summary Template;
- 360° feedback Report Template
- End of Test Attestation Template.

Outputs:

- RT Test Report;
- BT Report;
- Remediation Report;
- TIBER-BE Test Summary;
- Information shared with other institutions on test outcomes;
- 360° feedback report
- Signed End of Test Attestation.

6.3 RT Report and BT / RT Replay

It is recommended that the detailed RT test report and actual playbook of the RT test stay within the Concerned Insitution and can only be consulted on-site by authorized individuals.

After the RT delivers its RT test report, the Concerned Institution arranges a replay workshop. The goal of this workshop is to learn about the testing experience in collaboration with the RT provider. During the workshop a replay is organised in which the BT and the RT review the steps taken by both parties during the Test. Additionally, a purple teaming element is added in which the BT and the RT can work together to see which other steps could have been taken by the RT and how the BT could have responded to those steps. The TIBER-BE representative is also present during these replay and purple workshops.

During the replay meeting, the RT provider should express this in terms of how far the testing team, as threat actor mimics, managed to progress through the targeted attack life cycle stages of each threat scenario. The RT provider should also offer an opinion as to what else could have been achieved with more time and resources, as genuine threat actors are not constrained by the time and resources limitations of TIBER-BE.

6.4 360° feedback

During the 360° feedback meeting, the Concerned Institution, TBT, TIand RT providers come together to review the TIBER-BE exercise. The TBT arranges and facilitates the workshop. In the 360° feedback report, all parties deliver feedback to each other. Goal is to further facilitate the learning experience of all those involved in the process for future exercises.

6.5 Remediation plan, TIBER-BE TEST Summary, and sharing of results

After the BT and RT replay, purple teaming and 360° feedback workshops, the Concerned Institution should work on its remediation plan and the TIBER-BE Test Summary.

Based on the test outcomes, the Concerned Institution can work on a remediation plan. The TIBER-BE documentation can be used to support the business case for implementing improvements to mitigate the vulnerabilities identified during the TIBER-BE test.

The TIBER-BE Test Summary summarises the TIBER-BE process and should draw upon the delivered documentation such as the RT- and BT reports, the threat actor intelligence, the target intelligence and its remediation plan.

Since the TIBER-BE test focuses on the Belgian Critical Market Infrastructures and Core Financial Institutions as a group, sharing of information between the Concerned Institutions is also part of the TIBER-BE framework. As one of the main goals of TIBER-BE is enhancing the sector's resilience against advanced cyber attackers and financial stability, the participating Concerned Institution shares specific information regarding weaknesses with relevant peers promptly to enhance the cyber resilience of the sector and financial stability.

The Concerned Institution can share more general lessons learned via the TIBER-BE Test Summary. The TBT and the WT will discuss the forum for sharing the information, and the level of detail.

The gathered intelligence and lessons learned from the test will be input for the GTI used in future tests.

6.6 Supervision

The TBT does not share TIBER-BE-related information or documentation regarding a specific Concerned Institution with the NBB's Supervision or Oversight departments during the exercise. After the TIBER-BE process has been completed (the TIBER-BE Test Summary has been delivered), the TBT notifies the supervisor or overseer that the test has ended. It is recommended that the Concerned Institution addresses the TIBER-BE test in its regular planning and control cycle meetings with its supervisor or overseer.