TIBER-NL GUIDE

How to conduct the TIBER-NL test

November 2017

TIBER-NL GUIDE 2.0

Contents

1. Introduction

1.1 Background

Institutions that comprise the Dutch Financial Core Infrastructure (FCI) must remain resilient to cyberattacks causing systemic impact. To help achieve this goal, the Financial Stability Committee has commissioned De Nederlandsche Bank (the Dutch Central Bank/DNB) to lead the implementation of a framework for Threat Intelligence-based Ethical Red teaming: the TIBER-NL framework. The implementation of the framework is a joint effort of all FCI institutions and officially started on 30 June 2016.

Within the TIBER-NL framework, FCI parties hire cyber security providers to deliver controlled test attacks on their live critical core systems. Of course, the integrity, confidentiality and availability of the operational processes will be safeguarded during the test.

TIBER tests mimic potential attacks from real threat actors. The test mimics high level threat groups only (organised crime groups / state proxy/ nation state attackers) and thereby tests whether defensive measures taken are effective (capability assessment), supplementing the present periodic information security audits (process assessments) by e.g. supervisors and overseers. The tests also supplement current penetration tests and vulnerability scans executed within FCI parties. Test scenarios will draw on current commercially obtained threat intelligence that will where possible be enriched and reviewed with Governmental Intelligence (GI). This testing method aims to determine, and importantly serves to improve the capabilities of targeted institutions. The TIBER-NL framework is intended to improve their cyber resilience and ultimately, the cyber resilience of the FCI as a whole. TIBER-NL 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). As such, the BT is unaware of the TIBER-NL test. The actual test consists of time boxed phases (recon, in, through, out). As a consequence existing controls, prevention measures, and security detection and response capabilities against advanced attacks can be tested throughout all phases of the attack. It also helps identify weaknesses, errors or other security issues in a controlled manner.

The test phase is followed by full disclosure and a replay (that may include purple teaming) between the Red Team and the Blue Team to identify gaps, address findings and improve the response capability. During the test a White Team consisting of only the smallest necessary number of the FI'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 White Team will be in close contact with the TIBER-NL Test Manager from DNB's TIBER-NL Cyber Sector Team (TCST), who convoys the TIBER-NL test process.

Collaboration, evidence and improvement lie at the heart of TIBER. What differentiates TIBER from other security tests is its intelligence-led holistic approach and FCI focus. This means that financial institutions can improve their resilience based on proven relevant weaknesses rather than on perceived / possible weaknesses. This means TIBER delivers a higher return on security investments than solely working from a compliance-driven risk framework and defending against perceived risks. In addition, the central role of DNB's TCST enables comparison and the distillation of best practices in the FCI. The TIBER method can also be applied in other critical infrastructure sectors.

1.2 Purpose of this guide

This guide has been developed by the TCST from the Dutch Central Bank in close cooperation with all institutions from the Dutch FCI. It is meant to serve these TIBER-NL participants and their cyber security service providers. It explains the key phases, activities, deliverables and interactions involved in a TIBER-NL test.

This document is a guide rather than a detailed prescriptive method. It should therefore be consulted alongside other relevant TIBER-NL materials which will be provided by the TCST to TIBER-NL participants. This guide only details the TIBER-NL test process. How to implement a TIBER program is not detailed. The TCST is available to answer any questions that Institutions or cybersecurity service providers might have on the TIBER-NL test process or the TIBER-NL program.

1.3 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 shall accept no 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 within it.

- ShareAlike — If you remix, transform, or build upon the material, you must distribute your contributions under the same license as the original.
- No additional restrictions — you may not apply legal terms or technological measures that legally restrict others from doing anything the license permits.

Notices:

- You do not have to comply with the license for elements of the material in the public domain or where your use is permitted by an applicable exception or limitation.
- No warranties are given. The license may not give you all of the permissions necessary for your intended use. For example, other rights such as publicity, privacy or moral rights may limit how you use the material.

2. TIBER-NL overview

2.1 Introduction

This section provides an overview of the TIBER-NL test process.

2.2 Stakeholders

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

- A Financial Institution (FI) that is part of the Dutch Financial Core Infrastructure (FCI), only the White Team (led by the White Team Lead (WTL) knows about the test;
- The TIBER-NL Cyber Sector Team (TCST) of De Nederlandsche Bank (DNB);
- The Red Team provider (RTP) & (optional) the Threat Intelligence Provider (TIP)

2.3 Process overview

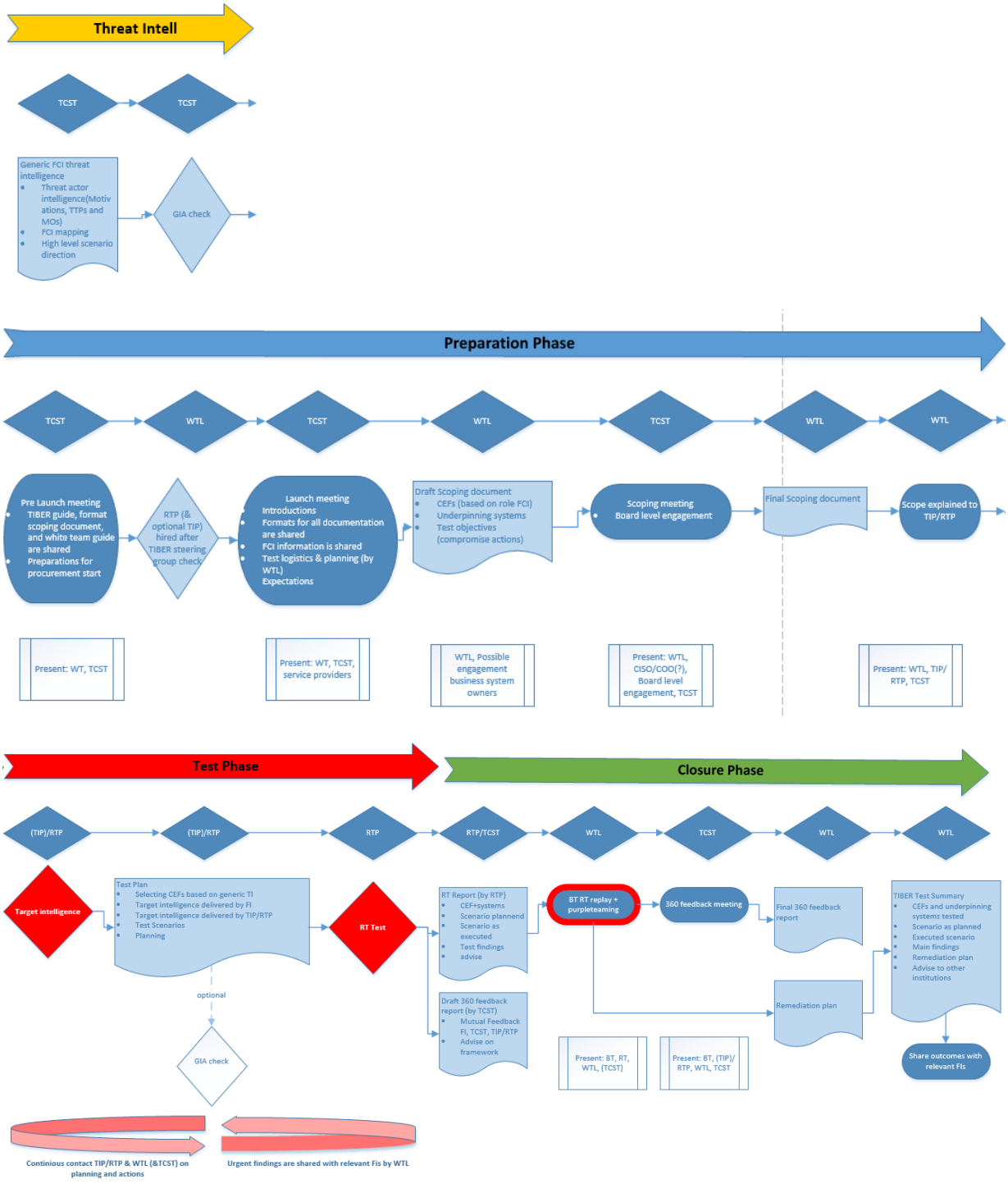
The TIBER-NL test process consists of four phases:

1. **The Generic FCI Threat Intelligence** shows the role of the commissioning FIs in the FCI (investment banks, commercial banks, CCP and exchanges), the threat actors (including their TTPs and MOs) and the expected threat actor motivations. This document will where possible be enriched and reviewed with Governmental Intelligence (GI).
2. **The Preparation Phase** during which the TIBER-NL test is formally launched, the White Team is established, the scope is determined and attested to, and a Red Team Provider is procured. Optionally a Threat Intelligence provider is procured;
3. **The Test Phase** during which the Red Team Provider or a Threat Intelligence Provider enriches target intelligence, and the RTP 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. **The Closure Phase** during which a replay of the executed scenarios will take place between the Blue Team and the Red Team, the FI's Remediation Plan is finalised. The process is reviewed and detection and response capabilities are assessed. Findings will be shared with peers if the benefit is greater than the risk. FI's inform their respective Supervisor or Overseer about the TIBER-NL test in their regular meetings.

The process model on the next page is a logical depiction of the TIBER-NL process. However, in reality the process is not such a neat linear sequence of steps: some activities may start earlier and run in parallel with others in order to increase efficiency given the limited timescales of the test. The TCST Test Manager will help by advising the White Team Lead (WTL) on the timing of the test phases in order to generate synergy.

The first phase, the generic FCI threat intelligence process will be executed by the TCST for all of the tests. The outputs will be shared with the institutions. The next three phases (preparation, testing and closure) will be dealt with separately per institution.

Figure 2.1 TIBER-NL test process model



2.4 Test management

The TCST Test Manager (TTM)

The role of the TTM is to make sure FIs undergo tests in a uniform and controlled manner. During all phases of the TIBER-NL process, the FI's White Team closely cooperates with the TTM. The TTM convoys the White Team through the TIBER-NL phases, but can in no way be held accountable for the White Team's actions or any TIBER-NL test consequences for the participating FI. The TTM has a close relationship with the White Team but is not formally part of the team. S/he has a right to escalate (major) deviations from the set

test scope or scenario to the TIBER-NL program manager, to whom s/he directly reports. The TCST program manager can escalate to the CISO of the FI, the TIBER-NL commissioner from DNB can escalate to the COO from the FI. Of course, escalation should be a last resort.

The TIBER-NL test manager will:

- Align closely with the White Team lead to make sure the test follows the agreed procedure and meets the right quality level for a TIBER-NL Test,
- Make sure the individual tests fit the function of the FI in the FCI, 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 RTP and possibly the TIP during the test
- Develop international cooperation with other TIBER-NL-like programs regarding testing,
- R&D regarding testing and talent development,
- Continuously develop the TIBER-NL framework based on experiences during the tests.

Responsibilities TCST Test Manager and FI White Team Lead (WTL)
The responsibility for the overall planning lies with the FI. The WTL within the FI coordinates all activity including engagement with the service provider(s). Service provider(s) produce a planning for their services and inform the FI so they can be factored into the overall TIBER-NL test project planning of the FI. Significant deviations in the original planning will be discussed with the TCST Test Manager as s/he will have several FI tests running simultaneously. The TCST can have direct access to the service providers when needed.

The TCST Test Manager agrees on the scope, the scenarios, ensures the test is executed according to plan and that it is up to the standards of a TIBER-NL test. There will have to be close cooperation between the TCST Test Manager and the White Team lead, with respect for individual roles and responsibilities. When there are crucial decisions to be made (e.g. deviations during the test from the scope agreed on) or unclarities or differences of opinion arise, the TIBER-NL Test Manager will be involved. Both the TCST and the FI undergoing the test will have a formal escalation line to their respective superiors in case of insurmountable divergent views. Usually these formal lines will consist of:

- The DNB TIBER-NL program manager, the division director responsible for TIBER-NL and the DNB board member responsible for TIBER-NL.
- The FI's White Team lead reporting to the CISO and to the COO.

TIBER-NL tests are to be a learning experience so are best underpinned by a collaborative, transparent and flexible working approach by all parties involved.

2.5 Managing the risks involved during the test

There are inherent elements of risk associated with a TIBER-NL test for all parties due to the criticality of the target systems, the people and the processes involved in the tests.

The FI makes sure when hiring service provider(s) (whether a Red Team Provider or a Threat Intelligence Provider) that there is mutual agreement on at least the following aspects: the scope of the test, boundaries, timing and availability of the providers, contracts, actions to be taken and liability (including insurance where applicable). A peer-check with the TIBER-NL Steering Group on the service provider(s) involved in a TIBER-NL test is another measure designed to further mitigate the risk of damage to critical live systems. In addition, close involvement of the TCST Test Manager in each TIBER-NL 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 on the test and the scope of the test, a clear definition of the scope and predefined escalation procedures. Importantly, the FI remains in control of and responsible for the red teaming test. At any time, the White Team can order a temporary halt if concerns are raised over damage (or potential damage) to a system. Trusted contacts within the White Team (see Section 3.4) positioned at the top of the security incident escalation chain help prevent miscommunication and knowledge about the TIBER-NL test leaking out.

The testing is to be flexible enough to mimic the (seen, current and potential future) actions of a real attacker *and* is to 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 FI 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
- Jeopardizing continuity of critical services
- Blackmail
- Threatening or bribing employees
- Disclosure of results

3. Generic Threat Intelligence

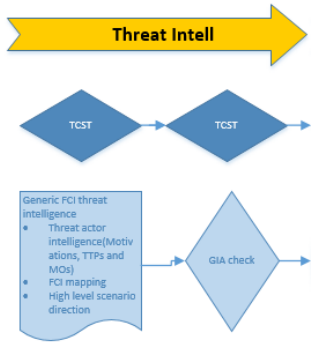
3.1 Overview

Generic Threat Intelligence will be provided by the TCST. During the Later Test Phase (chapter 5) the participating FIs will support the Red Team Provider (RTP) in connecting this generic TI to the scoping and the target intelligence. This is detailed in section 5.2. This third chapter is kept short as it does not describe a process that is to be followed by the FI.

The Generic Threat Intelligence consist of:

- Threat actor intelligence on the most advanced actors relevant for the Dutch Financial Institutions (FI's) in the Financial Core Infrastructure (FCI)
- Additional information regarding the position of the FI within the FCI and its corresponding CEFs that may be of interest to advanced attackers (threat actor aims);

Figure 3.1 TIBER-NL Threat Intelligence on advanced attack groups



Relevant documents

- The Generic FCI Threat Intelligence document is provided by the TCST

Output of this phase:

- Input for the Preparation Phase (specifically it will provide input for the launch meeting, the scoping document and the Targeting Report).

3.3 Governmental Intelligence

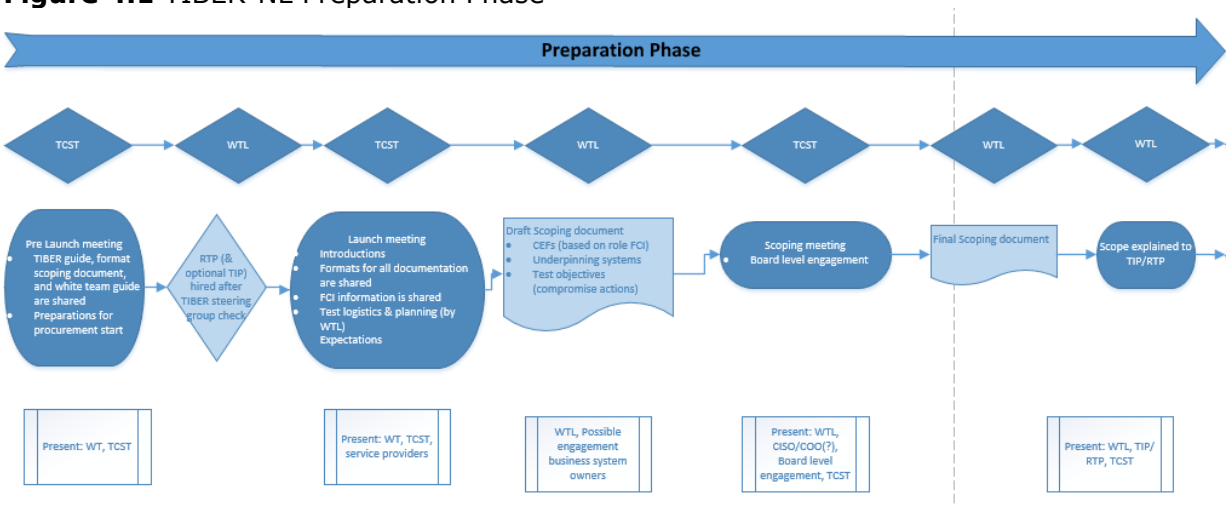
Governmental parties involved in the TIBER-NL program are the National Cyber Security Center, the National Police's Team High Tech Crime, the General Intelligence Agency and the Military Intelligence Agency. These parties will where possible validate and enrich the commercial threat actor intelligence provided and the high level scenarios. Optionally they can also perform a check on specific target information (e.g. threats, scenarios) for an FI in the Preparation Phase.

4. Preparation Phase

4.1 Overview

During the TIBER-NL Preparation Phase the project is formally launched and the TCST Test Manager starts engaging with the participating FI. The scope is established and the FI procures the service provider(s). The duration of this phase of work is approximately 4–6 weeks, not including the duration of the FI's procurement process. An overview of the key activities involved in this phase is shown in Figure 4.1.

Figure 4.1 TIBER-NL Preparation Phase



Relevant documents

- Ideal White Team lead
- Services Assessment Guide
- White Team Guidance
- Format Scope Specification
- Generic FCI intelligence document (on threat actors, FCI mapping and suggested scenario's)

Outputs of this activity are:

- TIBER-NL Test Scope produced by the FI for delivery to the TCST and service provider(s);
- TIBER-NL Project Planning produced by the FI for delivery to the TCST and service provider(s)

4.2 Pre-launch and Procurement

The pre-launch meeting marks the start of the planned and agreed on TIBER-NL process for each individual FI. The TIBER-NL Test Manager asks the FI to establish a White Team. 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 White Team Lead will make sure they are aware of the TIBER-NL red teaming test, the need for secrecy and the process the team should go through in case the Blue Team detects and escalates a TIBER-NL related incident. The launch session will be held with the White Team lead and additional White Team members as the lead sees fit. During the launch session, the TTM briefs the FI on requirements for:

- the TIBER-NL process and documentation
- stakeholder roles and responsibilities
- contractual considerations
- project planning

With regard to contractual considerations, smooth delivery of a TIBER-NL test requires that the process is transparent and appropriate information and documentation flows freely between the relevant parties. To facilitate the free flow of information, participating parties can sign a Non-Disclosure Agreement (NDA).

After the pre-launch meeting, the FI starts its procurement process. The FI then selects a Red Team Provider (RTP) to perform the test. Importantly, the FI offers a shortlist of potential providers to the TIBER-NL Steering Group and receives a recommendation regarding the providers. Optionally, the FI can also procure a Threat Intelligence Provider (TIP).

During Procurement the FI undertakes the following activities:

- Procures and takes onboard an RTP and (possibly) a TIP, ensuring that it has incorporated the NDA clauses into its service provider contracts;[1]
- Confirms and agrees the scope with the TCST and completes the TIBER-NL Scope Specification;
- Completes the TIBER-NL Test Project Plan, including the final schedule of meetings to be held between the FI, RTP, and TCST.

4.3 Launch

Since cooperation is key for a successful TIBER-NL 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-NL Project Planning.

4.4 Scoping

During the launch, the TCST provides the FI with a Scope Specification format. The FI then starts work on a draft version of the TIBER-NL Scope Specification. The TIBER-NL Test Manager is available during the scoping process to clarify the requirements and is available to give feedback. The TIBER-NL Scope Specification defines the scope of the TIBER-NL test, specifically the Critical Economic Functions involved. Within the TIBER-NL framework Critical Economic Functions (CEFs) are defined as the people, processes and technologies required to deliver a core service which, if disrupted, could have a detrimental impact on the Dutch financial stability, the firm's safety and soundness, the firm's customer base or the firm's market conduct.

Note that a CEF is not a system. It is a function which could be considered critical or essential to the Financial Services sector and/or to a Financial Services sector organisation. FIs across the sector support and deliver these functions in different ways via their own internal processes which are in turn underpinned by critical technological systems. It is these critical technological systems, processes, and the people surrounding them, that are the focus of TIBER-NL threat intelligence and red teaming. Flags are placed on the critical systems in the scope document. These flags form the goal for the later test scenarios which are based on relevant threat intelligence. The FI is allowed to involve the RTP (and TIP if hired) in the scoping process.

4.5 Scoping meeting

The final scope document is agreed on by the TCST Test Manager during a workshop organised by the FI. Importantly, the scoping will need to be agreed on at board level of the FI (attestation). Further information on the TIBER-NL Scope Specification can be found in the TIBER-NL Scope Specification document.

[1] The TIBER test cannot proceed beyond Procurement until the FI has checked and provided an attestation that appropriate legal contracts are in place between the FI and the TI/RT service providers. This is particularly key for the RTP to ensure it has the relevant permission to conduct testing against the systems in scope so that it is not found to be in breach of relevant legislation.

4.6 Scope explained to TIP/RTP

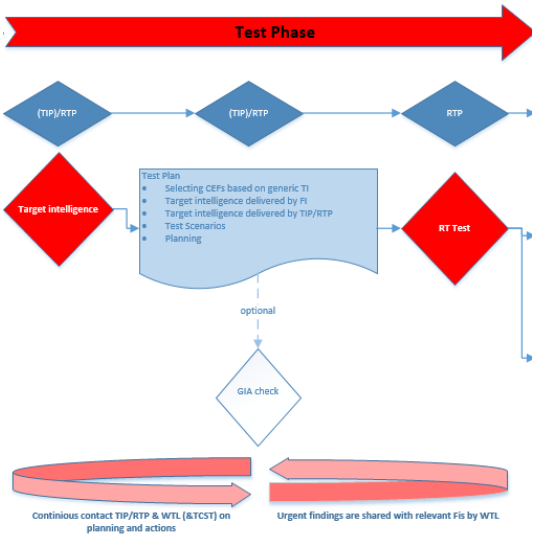
For a successful test it is important that the service providers understand the business of the FI. Therefore, after the scoping and in case the service providers were not already involved during the scoping, a meeting is planned with the provider(s) in which the CEFs and systems underpinning them (compromising these is the test objective) are explained. If the FI feels that further interaction on 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 FI, the detailed test scenarios are built and the red team test is executed. These scenarios will be built by the Red Team provider in the Test plan. If urgent findings relating to vulnerabilities relevant to other FIs are found, these are shared. An overview of the key activities involved in this phase is shown in Figure 5.1.

Figure 5.1 Test Phase



Relevant documentation

- Format Test Plan
- Generic FCI intelligence document

Output of this phase

- Test Plan
- RT Test

5.2 Target Intelligence delivered by the RTP/TIP

In this phase, either the TIP or the RTP can execute an initial furtive broad, intelligence-based targeting exercise of the kind typically undertaken by threat actors as they prepare for their attack. The objective is to draw a picture of the FI as a target from the attacker's perspective. The use of various methods (including OSINT, TECHINT, HUMINT, and intelligence-based initial targeting) is encouraged.

The output of the Target Intelligence identifies, on a CEF-focused, system-by-system basis, the people, processes and infrastructure relating to the FI. This includes information

that is intentionally published by the organisation or about the organisation 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 Target Intelligence delivered by the RTP/TIP will contribute to the development of the test scenarios.

5.3 Test Plan

In the Test Plan, the RTP will put together attack scenarios for the RT Test which:

- Map onto one or more Critical Economic Function-supporting systems;
- Combine the Threat actor intelligence (TCST) and Target Intelligence (FI + RTP/TIP) and aligns these into credible scenarios;
- Provides background to the tradecraft of the type of actor that is mimicked in the attack;
- Provides creative elements of what TTPs that have not yet been seen in the wild but that are according to the professional knowledge of the RTP to be expected for the future;
- Would, if occurring in real life, have a destabilising effect on the Dutch financial stability;
- Also provide some elements which test the response of the FI, including evidence on whether the compromise action would be immediately detected or could have a fair chance of succeeding.

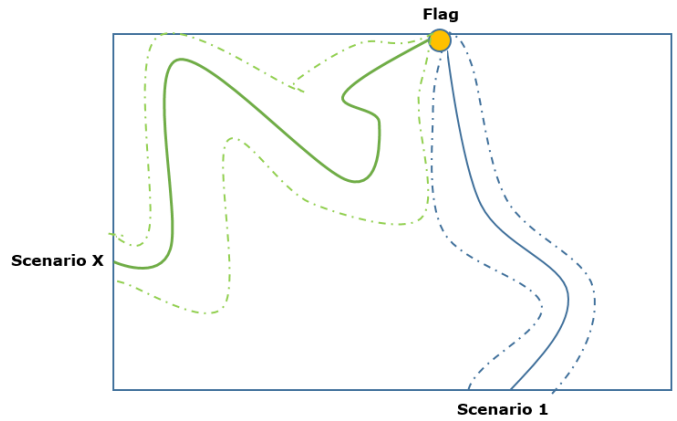
Scenarios

Scenarios should are built based on the general TIBER-NL threat intelligence document, the scoping and targeting information of the previous sections.

The scenarios are written from the attacker's point of view. The RTP indicates various creative options in each of the attack phases based on various tactics, techniques and procedures used by advanced attackers, to anticipate changing circumstances or if the first option does not work. The scenario writing is a creative process. The TTPs do not only to mimic those seen in the past, but combine techniques of the various relevant threat actors.

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

Figure 5.2 Scenarios and scenario X



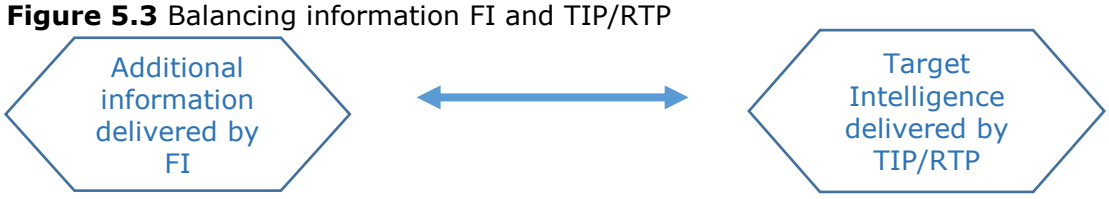
Additional information delivered by the FI
The FI delivers additional information for the RTP on the scenarios chosen including on people, processes and systems targeted in the scenario. The level of detail of this information is up to the FI to decide.

The TIBER process is designed to create realistic threat scenarios mimicking possible future attacks against the FI. 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-NL service providers must observe, such as the time and resources available – not to mention the moral, ethical and legal boundaries.[2] 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 critical economic functions 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 an RTP may be limited in comparison to those attackers with the capacity and time to study these extensively.

Therefore, it depends on the FI how much information it is willing to give to make sure the RTP is on the right level of knowledge to mimic advanced attacks. This way, TIBER reflects a 'grey box' testing approach in contrast with the 'black box' approach. The RTP receives support from the FI 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 RTP 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 RTP could have been obtained by an advanced attacker, given more time, different known techniques etc. Whether this information is provided by the FI or delivered by a Third Party TIP, is up to the FI.

Figure 5.3 Balancing information FI and TIP/RTP



The above model shows the balance between target information delivered by the FI or TIP/RTP. More of one means less is needed from the other, and time can be spent elsewhere (for the RTP this will mean relatively more actual test time).

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 RTP to be able to work in a stealthy manner.

2 It is up to the FI to set up contractual agreements with the RTP 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.

Based on the Test Plan, the TCST decides, on the basis of the FI's request, if an extra GIA check is necessary.

5.3 Test

The Red Team Provider (RTP) now moves into execution of the Red Team Test during which the RTP performs a stealthy intelligence-led red teaming exercise against the target systems. The RT Test takes approximately 12 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 RTP 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 White Team and the TIBER-NL test manager (TTM). All actions of the Red Team are logged for replay with the Blue Team, evidence for the Red Team Report and future reference.

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

RTPs are constrained by the time and resources available as well as moral, ethical and legal boundaries. It is therefore possible that the RTP may require occasional steers from the White Team to help them progress. Should this happen, then these steers are duly logged. This ensures that maximum benefit is derived by all stakeholders from a time-limited test.

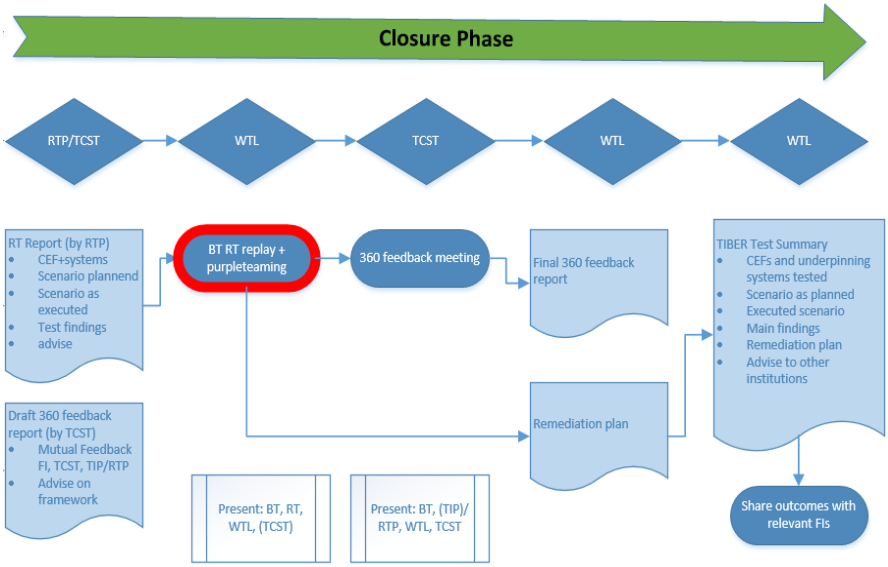
At all times the RTP liaises closely with the FI's White Team and with the TTM. The TTM is updated at least once a week by the RTP and White Team on the progress. Physical meetings between the White Team, TTM and Red Team during this phase are strongly encouraged since the discussions add significantly 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.

Figure 6.1 Closure Phase



The output of this activity is a draft version of the Red Team Test Report produced by the RTP for delivery to the FI who then forwards the document to the TCST. The draft report must be issued within two weeks of test completion. The FI's Blue Team is informed of the test and will use the Red Team Test Report to deliver its own Blue Team report. In the Blue Team report, the Blue Team maps its actions alongside the Red Team actions.

Relevant documentation

- Format Red Team Test Report
- Format TIBER-NL Test Summary
- Format 360 feedback Report

Outputs

- Red Team Test Report
- Blue Team Report
- Remediation Report
- TIBER-NL Test Summary
- Information shared with other FIs on test outcomes
- 360 feedback report

6.2 RT Report and Blue Team/Red Team Replay

After the Red Team delivers its report, the FI arranges a replay workshop. The goal of this workshop is to learn about the testing experience in collaboration with the RTP. During the workshop a replay is organized in which the Blue Team and the Red Team review the steps taken by both parties during the Test. Additionally, a purple teaming element can be added in which the Blue Team and the Red Team can work together to see which other steps could have been taken by the Red Team and how the Blue Team could have responded on those steps. The TIBER-NL Test Manager can also be present during this replay workshop.

6.4 360 feedback

During the 360 feedback meeting, the FI, TCST, (TI-) and RT service provider(s) will come together to review the TIBER-NL exercise. The TCST arranges and facilitates the workshop. In the 360 feedback report all parties deliver feedback on each other. Goal is to further facilitate the learning experience of all those involved in the process for future exercises.

When reviewing the results of the test during the 360 feedback meeting, the RTP 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 RTP should also offer an opinion as to what else could have been achieved with more time and resources given that genuine threat actors are not constrained by the time and resources limitations of TIBER-NL.

6.3 Remediation plan, TIBER-NL TEST Summary, and sharing of results

After the Blue Team and Red Team replay and 360 feedback workshop, the FI should work on its remediation plan and the TIBER-NL Test Summary.

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

The TIBER-NL Test Summary summarises the TIBER-NL process and should draw upon the delivered documentation such as the Red Team- and Blue Team reports, the threat actor intelligence, the target intelligence and its remediation plan.

Since the TIBER-NL test focuses on the FCI as a group, sharing of information between the FIs is also part of the TIBER-NL framework. As one of the main goals of TIBER is enhancing the sector's resilience against advanced cyber attackers, the participating FI shares specific information regarding weaknesses with relevant peers promptly to enhance the cyber resilience of the sector. The FI can share more general lessons learned via the TIBER-NL Test Summary. The TCST and the White Team can 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 generic threat intelligence used in future tests.

6.5 Supervision

The TCST will not share TIBER-NL-related information or documentation regarding a specific FI with DNB's Supervision or Oversight departments during the exercise. After the TIBER-NL process has been completed (the TIBER-NL Test Summary has been delivered), the TCST will notify the supervisor or overseer that the test has ended. It is recommended that the FI addresses the TIBER-NL test in their regular planning and control cycle meetings with its supervisor or overseer.

7. Annex I: Abbreviations used in this document

Term	Explanation
BT	Blue Team
BTR	Blue Team Report
CBEST	The Bank of England cyber resilience program on which TIBER-NL is based
CREST	Council for Registered Ethical Security Testers (www.crest-approved.org)
DNB	Dutch Central Bank (De Nederlandsche Bank)
FCI	Financial Core Infrastructure
FI	Financial Institution
GI	Governmental Intelligence
NCSC	National Cyber Security Center
OSINT	Open Source Intelligence
RT / RTP	Red Teaming / Red Teaming Provider
TCST	TIBER-NL Cyber Sector Team
TI / TIP	Threat Intelligence / Threat Intelligence Provider
TIBER	Threat Intelligence Based Ethical Red teaming
TTP	Tactics, Techniques and Procedures used in a cyber attack
TTM	TIBER Test Manager
WT	White Team
WTL	White Team Lead

8. Annex II: Relevant documentation – an overview

All documents are 'living' documents. After the first TIBER-NL testing period drafts have been developed for the second testing round. Each future round or development will possibly lead to revision of the TIBER-NL documentation. The TIBER-NL process must always be agile enough to adapt to the evolving threat landscape.

Preparation Phase

- Ideal White Team Lead
- White Team Guidance
- Services Assessment Guide
- Format Scope Specification

Test Phase

- Format Test Plan

Closure Phase

- Format Red Team Test Report
- Format 360 Feedback Report
- Format TIBER-NL Test Summary