TIBER-NL GUIDE
How to conduct the TIBER-NL test

January 2020

TIBER-NL GUIDE 3.0

Traffic Light Protocol: white

Contents

1. Introduction

1.1 Background

Institutions that comprise the Dutch Financial Sector must continuously work on their resilience against cyberattacks causing systemic impact. To help achieve this goal, the Dutch Financial Stability Committee has commissioned De Nederlandsche Bank (the Dutch Central Bank/DNB) to lead the development and implementation of a framework for Threat Intelligence-based Ethical Red teaming: the TIBER-NL framework. The development and implementation of the framework is a joint effort of the most critical Dutch financial institutions and officially started on 30 June 2016. TIBER-EU has been commissioned in 2018 by the ECB. This framework is leading and TIBER-NL is a derivative thereof. The aim of TIBER-EU is to make cross border testing of multinational financial institutions (FI) possible and make sure tests can be recognised by all the competent authorities of the Euro-system countries who have adopted TIBER-XX (and also under some conditions by countries with similar testing frameworks like CBEST in the UK). The TIBER method has proven to be applicable in other critical infrastructure sectors.

Within the TIBER-NL framework, FI hire cyber security providers to deliver intelligence and controlled simulated attacks on their live critical production systems. Procedures and safeguards will be put in place to minimize the risk to the integrity, confidentiality and availability of the operational processes.

TIBER tests mimic potential attacks from real threat actors. The test emulates high level threat groups only (organised crime groups / state proxy/ nation state threat actors) and thereby tests whether defensive measures taken are effective (capability assessment), "supplementing the present work done by supervisors and overseers. The tests also supplement current penetration tests, red teaming exercises and vulnerability scans executed within entities. Test scenarios will draw on current commercially obtained threat intelligence that will where possible be enriched and reviewed with Governmental Intelligence Agencies (GIA). This testing method aims to determine, and importantly serves to improve the cyber resilience capabilities of targeted FI. The TIBER-NL framework is intended to improve their cyber operational resilience and ultimately, the cyber operational resilience of the financial sector 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 (reconnaissance, 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 to the BT and a replay (which has to include purple teaming) between the Threat Intel Provider (TIP, Red Team Provider (RTP) and the institutions BT to identify gaps, address findings and improve the response capability. During the test a White Team (WT) consisting of only the smallest necessary number of people from the FI security and business units. They 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 TIBER-NL Test Managers (TTM) from DNB's TIBER-NL Cyber Team (TCT), who convoys the TIBER-NL test process.

Collaboration, evidence and improvement lie at the heart of TIBER. What differentiates TIBER-NL from other security tests is its intelligence-led holistic approach and financial sector focus in which collaboration and learning are central elements. This means that FI can improve their resilience based on proven relevant weaknesses rather than on perceived / possible weaknesses. This means TIBER-NL 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 TCT enables comparison and the distillation of best practices in the FCI and the pension and insurance sector.

1.2 Purpose of this guide

This guide has been developed by the TCT from the Dutch Central Bank in close cooperation with all participants of TIBER-NL and is a derivative of the leading TIBER-EU framework. 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, TIBER-XX and TIBER-EU materials which will be provided by the TCT to TIBER-NL participants. This guide only details the TIBER-NL test process. How to implement a TIBER program is not detailed. The TCT is available to answer any questions that FI or cyber security 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.

2. TIBER-NL overview

2.1 Introduction

This section provides an overview of the TIBER-NL test process. Focus of this guide is on tests on a single entity within the Netherlands. Tests can also include 3rd parties, supply chain and cross border testing within the Euro-system countries. The Dutch TCT has experience with and can advise on these tests.

2.2 Stakeholders

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

- an FI that is part of the Dutch Financial Core Infrastructure (FCI) or the pension or the insurance sector> Within the FI only the White Team (led by the White Team Lead (WTL) knows about the test;
- the TIBER-NL Cyber sector Team (TCT) of De Nederlandsche Bank (DNB);
- the Red Team provider (RTP);
- the Threat Intelligence Provider (TIP);
- governmental Intelligence Agencies (GIAs);
- third party service providers (e.g., outsourcing partners);
- other competent authorities.

2.3 Process overview

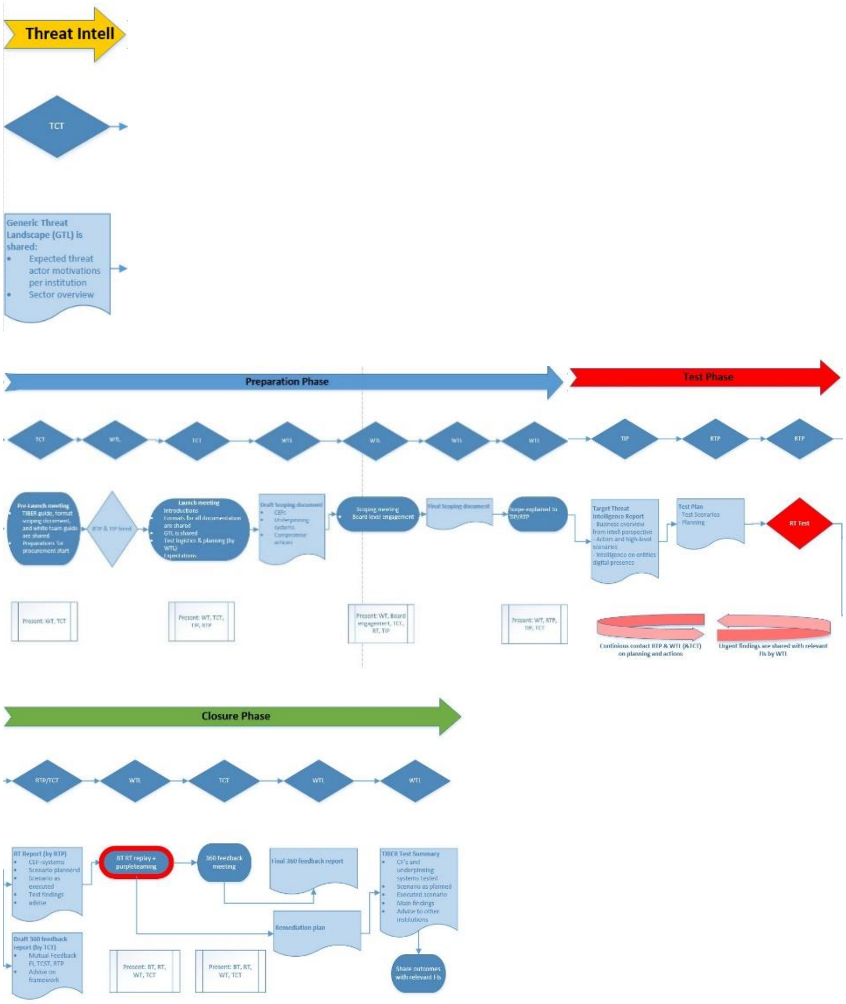
The TIBER-NL test process consists of four phases:

1. **The Generic Threat Landscape (GTL) Report (Sector Specific Intelligence)** shows which threat actors are relevant for the FI. It also shows the recent TTPs and Modus Operandi (MO) for these threat actors and reflects on the motivations to attack the critical functions of the institution. This document will where possible be enriched and reviewed with Governmental Intelligence Agencies (GIA).
2. **The Preparation Phase,** during which the TIBER-NL test is formally launched, the WT is established, the scope is determined, critical functions (CF) are defined and approved by the board, and a TIP and a RTP are procured. If the RTP is capable of providing target intelligence and producing intelligence led scenarios on the highest standards, then procuring a separate TIP is not mandatory. The RTP in that case needs to comply with the requirements of "Chinese walls" in scenario development between threat intelligence and red teaming phases.
3. **The Test Phase,** during which target intelligence is gathered and intelligence led scenarios are produced, 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 & Learning Phase,** during which a replay of the executed scenarios will take place between the BT, the TIP and the RT. The TIBER process is reviewed and the FI remediation plan is finalised. Good practices will be shared with peers by the entity if the benefit is greater than the risk. The FI inform their respective supervisor and / or overseer about the TIBER-NL test in their regular meetings based on their remediation plan following the test.

The process model below 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 TCT Test Manager will help by advising the WTL on the timing of the test phases in order to generate synergy.
The first phase, the generic threat intelligence process will be executed by the TCT for all of the tests. The output (Generic Threat Intelligence Report) will be shared with the FIs.

The next three phases (Preparation, Testing and Closure & Learning) will be dealt with separately per institution.

Figure 2.1 TIBER-NL test process model



2.4 Test management

The TCT Test Manager (TTM)

The role of the TTM is to make sure FI undergo tests in an uniform and controlled manner. During all phases of the TIBER-NL process, the FI WT closely cooperates with the TTM. The TTM convoys the WT through the TIBER-NL phases, but can in no way be held accountable for the WT actions or any TIBER-NL test consequences. The TTM has a close relationship with the WT 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 TCT program manager, to whom s/he directly reports.

The TCT Test Manager will:

- Align closely with the WTL 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 entity, the threat intelligence and high level scenarios provided.
- Involve a Threat Intelligence Advisor from the TCT during the TI phase to verify the quality of the target intelligence and the scenarios in the Targeted Threat Intelligence Report.

- Assess the level of the cyber security service providers, and the level of the work of the RTP and possibly the TIP during the test.
- Facilitate sharing and learning between the FI participating in TIBER.
- Develop international cooperation with other TIBER-NL(-like) programs regarding testing.
- R&D regarding intelligence, testing and talent development;
- Continuously develop the TIBER-NL framework based on experiences during the tests.

The White Team and the White Team Lead
The WT is the team within the FI which is responsible for managing the test from within the FI. The WT consists at least of the WTL, the CISO and a C-level executive, usually the COO. The members of the WT are the only ones aware of the test within the FI. The WT is not a predefined team but members can be added and removed as necessary depending on the phase and status of the test. A full description of the tasks and responsibilities of the WT and the WTL can be found in the TIBER-EU White Team Lead Guide.

Collaboration between the TCT Test Manager and entity White Team Lead
The responsibility for the overall planning lies with the FI. The WTL within the FI coordinates all activity including engagement with the cyber security service provider(s). The importance of the WTL is hard to overstate. Its knowledge, attitude, energy and enthusiasm can make or break a test. Cyber security service provider(s) produce a planning for their services and inform the entity so the planning of the cyber security service provider 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 TCT Test Manager as s/he will have several entity tests running simultaneously. The TCT can have direct access to the cyber security service providers when needed.

The TTM 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. When the quality of the test does not meet the standards, the TTM can remove the TIBER label from the test. It will therefore not be recognised (inter)nationally as a TIBER test. There will have to be close cooperation between the TTM and the WTL, 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), uncertainties or differences of opinion arise, the TTM will be involved. Both the TCT and the entity 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:

- DNB: The TCT program manager, the division director responsible for TIBER-NL and the DNB board member responsible for TIBER-NL.
- The FI WTL 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.

Further details on the role of WTL van be found in the TIBER-EU White Team Guidance.

Multi-Jurisdiction tests
In the case where an entity is participating in a TIBER program of multiple jurisdictions with a TIBER framework and an active TIBER Cyber Team, the lead TTM is provided by the central bank who is the main supervisor or overseer for the tested institution. It is the joint responsibility of the WTL and the TTM to make sure to involve all relevant TIBER schemes in the test. In collaboration it can be decided to inform overseers or supervisors who don’t yet have a TIBER scheme of the results of a test. For more detail on multi-jurisdictional tests please refer to the TIBER-EU Framework.

2.5 Managing the risks during the test

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

Before an FI engages in a TIBER-NL test they should conduct a thorough due diligence of (possible) in scope systems to ensure that at least backup and restoration capabilities are in place. Furthermore it is advised that the FI conducts a risk assessment with regards to the risks a TIBER-NL test poses and that these risks are taken into consideration and handled.

The FI makes sure when hiring cyber security service providers (whether a Red Team Provider and / 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 cyber security 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 TTM in each TIBER-NL test makes sure that the test proceeds according to the agreed test scope, scenario, planning and process as described in the cooperatively developed framework documents. Minimum requirements for cyber security service providers, both TIP and RTP, are described in the TIBER-EU Services Procurement Guidelines.

Risks are also reduced by planning, informing only a 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. It is import to note that the FI remains in control of and responsible for the test. At any time, the WT can order a temporary halt if concerns are raised over damage (or potential damage) to a system or business processes. Trusted contacts within the WT (see Section 2.4) positioned at the top of the (security) incident escalation chain help prevent miscommunication and knowledge about the TIBER-NL test leaking out.

To prevent TIBER-NL tests from leaking out, code names are used. These code names should be used throughout all documentation related to the TIBER-NL test. Codenames will be assigned by the TCT.

The testing is to be flexible enough to mimic the (seen, current and potential future) actions of a real threat actor *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. These elements are essential in order to make sure the entity and its peers can learn and evolve, not only using their own but all relevant results and findings.

As a result of the test it is possible that during a test the BT has reached a level of escalation where it starts to inform relevant authorities such as, but not limited to, police, intelligence agencies or data-protection agencies. The WT should at all times try and prevent this from happening. Authorities should not be burdened by a TIBER test. In case the WT be informed of an active escalation to third authorities, the test should immediately be stopped and measures should be taken to prevent the authorities to act on the incident escalation.

The following is prohibited in TIBER-NL (not an exhaustive list):

- unauthorised destruction of equipment;
- uncontrolled modification of data / programs;
- unauthorized jeopardizing continuity of critical services;
- blackmail;
- threatening or bribing employees;
- kidnapping;

- the use of names, logos or otherwise identifiable information of real people or companies.

For more details on this please refer to paragraph 5.3.

3. Generic Threat Landscape

3.1 Overview

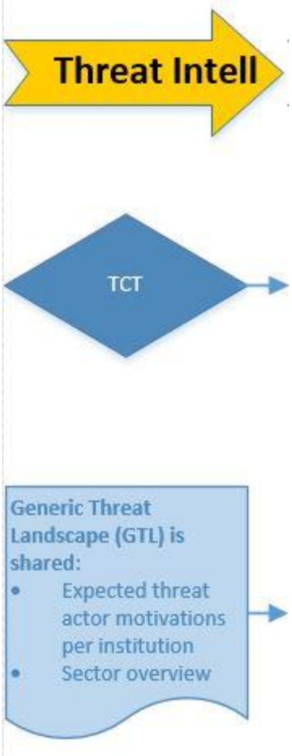
A Generic Threat Landscape Report for the purpose of the TIBER-NL test will be provided by the TTM. This chapter is kept short as it does not describe a process that is to be followed by the FI. During the later Test Phase (chapter 5) the FI will support the TIP and the RTP in connecting this GTL to the scope and the targeted threat intelligence. This is detailed in section 5.2.

Within each TIBER-NL test a Threat Intelligence Advisor (TIA) is appointed from the TCT, who will support the TTM in the beginning of the test and can challenge the TIP and RTP on the chosen scenarios.

The Generic Threat Landscape consist of:

- Threat intelligence on the most advanced actors relevant for the Dutch FI participating in TIBER-NL.
- Additional information regarding the position of the FI and its corresponding CFs that may be of interest to advanced threat actors (threat actor aims).

Figure 3.1 TIBER-NL Threat Intelligence on advanced threat actors



<u>Relevant documents</u>

- The GTL Report document is provided by the TCT.
- Access to an additional threat intelligence portal that ties in with the GTL is provided by DNB. Access to the portal is granted to the participating FI and the TCT.

Output of this phase:

- Input for the Preparation Phase and Test Phase (specifically it will provide input for the launch meeting, the TIBER-EU Scope Specification document, the Targeted Threat Intelligence Report and Test Plan).

3.3 Governmental Intelligence Agencies

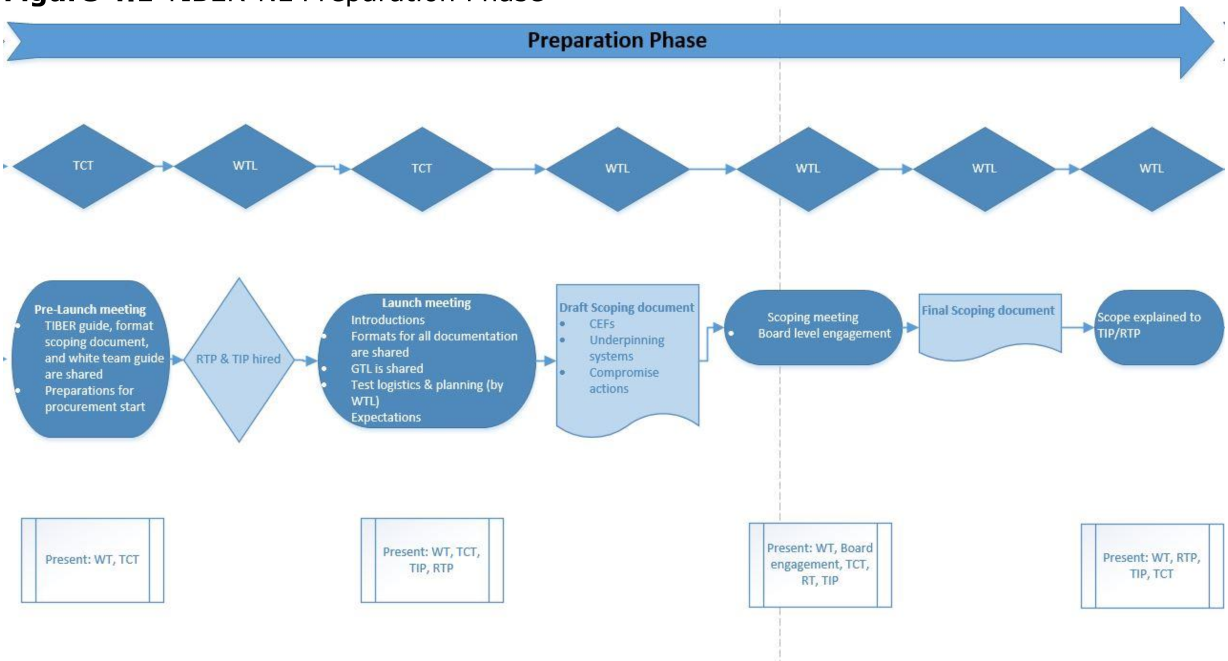
GIA's involved in the TIBER-NL program are the National Cyber Security Centre, the National Police's Team High Tech Crime, the General Intelligence Agency and the Military Intelligence Agency. These entities will where possible validate and enrich the Generic Threat Landscape provided and the high level scenarios. Optionally they can in addition 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 TTM starts engaging with the FI and the project is formally launched. The scope is established and the entity procures the cyber security service provider(s). The duration of this phase of work is approximately 4–6 weeks, not including the duration of the FI 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



<u>Relevant documents</u>

- TIBER-EU White Team Guidance;
- TIBER-EU Services Procurement Guidelines;
- TIBER-EU Scope Specification document;
- Generic Threat Landscape Report (on threat actors, FCI mapping and suggested scenarios).

<u>Outputs of this activity are:</u>

- TIBER-EU Scope Specification document produced by the entity for delivery to the TCT and cyber security service provider(s).
- TIBER-NL Project Planning produced by the FI for delivery to the TCT 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 the FI. The TTM asks the entity 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 they are aware of the TIBER-NL test, the need for secrecy and the process the team should go through in case the BT detects and escalates a TIBER-NL related incident. The TCT and the WTL jointly decide whether other jurisdictions of the FI will be included in the TIBER-NL test. This decision is made based upon in which countries the tested FI is part of the vital infrastructure. General rule is that if an FI is part of the vital infrastructure of a country and there is a TCT active in that country, the TCT from that country should be included in the test.

The launch session will be held with the WTL and additional WT members. During the launch session, the TTM briefs the entity on requirements for:

- the TIBER-NL process and documentation;
- other involved TCT members, such as second TTM and the TIA
- stakeholders, 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 must sign a Non-Disclosure Agreement (NDA).

After the pre-launch meeting, the entity starts its procurement process. The entity then selects a RTP and a TIP to perform the test. Importantly, the entity offers a shortlist of potential providers to the TIBER-NL Steering Group and receives feedback regarding the providers from the TTM.

During procurement the FI undertakes the following activities:

- Procures and takes on board a RTP and a TIP, ensuring that it has incorporated the NDA clauses into its cyber security service provider contracts.
- Completes the TIBER-NL Test Project Plan, including the schedule of meetings to be held between the FI, TIP, RTP, and TCT.

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 (at least the TTM, TIA, WT and RTP and TIP). During this meeting, all parties discuss the test process and their expectations. Also TIBER documentation is shared. They also discuss a draft TIBER-NL project planning. The project plan will be prepared by the WTL.

4.4 Scoping

During the launch, the TCT provides the entity with the latest version of the TIBER-EU Scope Specification format. The entity then starts work on a draft version. The TTM is available during the scoping process to clarify the requirements and is available to give feedback. The TIBER-EU Scope Specification defines the scope of the TIBER-NL test, specifically the critical functions involved. Critical Functions are defined as the people, processes and technologies required to deliver a core service which, if disrupted, could have an impact on the Dutch financial stability the firm’s safety and soundness, the firm’s customer base or the firm’s market conduct.

FIs across the financial sector support and deliver these functions in different ways via their own internal processes which are in turn underpinned by critical systems. It is these critical 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 TIBER-EU Scope Specification document. These flags form the goal for the later test scenarios which are based on relevant threat intelligence. The entity is allowed to involve the RTP and TIP in the scoping process. The TTM will involve supervision and / or oversight during the scoping to verify whether the scope is a realistic representation of the entity.

4.5 Setting and capturing the flags

During the scoping process, the entity must complete the TIBER-EU Scope Specification document. The TIBER-EU Scope Specification sets out the scope of the TIBER-NL test, and lists the key systems and services that underpin each CF. This information helps the WT set the "flags" to be captured, which are essentially the targets and objectives that the RTP must strive to achieve during the test.
The WT should discuss the flags with the TTM, who must approve them. Although the flags are set during the scoping process, in some occasions they can be changed following the threat intelligence gathering and as the test evolves.

4.6 Scoping meeting

The final scope document is agreed on by the TCT Test Manager during a workshop organised by the FI. Importantly, the TIBER-EU Scope Specification document will need to be approved at board level by one board member of the FI, usually this is the COO. This approval can be either a written approval or an oral approval with at least the WTL, TTM, RTP and TIP present.

In the case that an FI is tested for a second time and it is determined that the scope of the test is largely the same as the last test, the TTM and WTL can decide to have the board approve of the scenario's being played out.

4.7 Scope explained to TIP/RTP

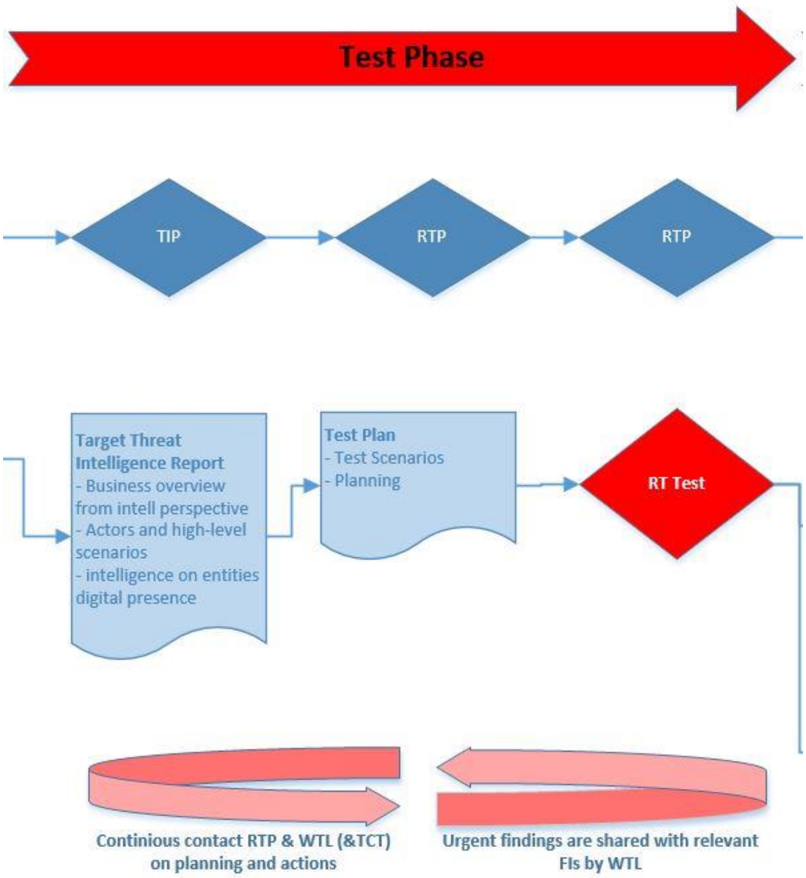
For a successful test it is important that the cyber security service providers understand the business of the FI. Therefore, after the scoping and in case the cyber security service providers were not already involved during the scoping, a meeting is planned with the provider(s) in which the CFs and systems underpinning them (compromising these is the test objective) are explained. If the FI feels that further interaction on the functioning of its business is necessary to arrive at realistic scenarios this is very much encouraged. The RTP and TIP should make sure they fully understand the scope, not only the technical details but also the business processes. If the RTP and/or TIP feels they need more guidance to understand the business processes of the FI, this should be provided by the WT who, in turn, can add specialists (temporarily) to the WT to provide the necessary information.

5. Test Phase

5.1 Overview

During the Test Phase target intelligence is gathered on the FI, these result in intelligence-led test scenarios. These scenarios will be expanded by the RTP into a Test Plan. If urgent findings are found to be relevant to other FIs, these will be 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 Threat Landscape Report;
- Format Targeted Threat Intelligence (TTI) Report;

Output of this phase

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

5.2 Targeted Threat Intelligence process

In this phase, the TIP executes 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 threat actors perspective.

The use of various methods (including OSINT, TECHINT, and intelligence-based initial targeting) is encouraged. It cannot be stressed enough that this phase is a passive phase. <u>No active reconnaissance should be undertaken</u>.

The targeted threat intelligence process results in the production of a TTI Report, which is a bespoke, focused threat intelligence report for the FI being tested. It consists of three parts:

1. A Business overview from an intelligence perspective.

This section is meant to provide a strategic understanding of the business of the FI and its current and planned activities. It also gives a more detailed insight into the business and systemic consequences of compromise of the Critical Functions.

To make the intelligence gathering as effective as possible the following information should be provided by the FI to the TIP:

- possible additional explanation about the core business of the FI, what is most critical for them and why is the FI vital for the broader landscape of institutions;
- a business and technical overview of each CF-supporting system in scope;
- the current threat assessment and/or threat register;
- examples of recent attacks.

The last two bullets are also used as an input for the TTI Report.

2. Actors and high level scenarios.

In this part the GTL will be further analysed by the TIP. Of relevant threat actors it will be determined how likely and capable they are to attack the specific entity their specific CFs. This will lead to a list of most likely and capable threat actors. These actors will form the basis for the scenarios. The TIP will write a high level scenario of how an attack by the specific threat actor would take place including with which motivation and intent the threat actor would attack specific CFs. Based on this the enrichment of the TTI Report contains the following items:

- most likely threat actors to target the CF of the FI;
- a motivation as to why exactly these threat actors;
- most likely targets for each threat actor;
- high level scenarios for the most likely threat actors.

3. Intelligence on entity's (digital) presence.

In this part the TIP provides the RTP with intelligence on what the threat actors included in scenarios would be able to get to know about the (digital) presence of the FI. It serves to provide more detail on how the threat actor would potentially attack the FI based on the opportunities laying in the (digital) presence.
In this section the FI can provide information to help focus the search of TIP.

The TTI report will be verified by the TIA of the TCT. The Target Intelligence delivered by the TIP will contribute to the further development of the test scenarios RTP.

Some key considerations for the TIP:

- TI providers must engage with the FI to obtain useful context for conducting the threat analysis. Although the FI may not always be able to share the details of sensitive incidents with the TIP, it should still be possible to learn about the FI both through engagement with the key stakeholders and by gathering evidence of previous breaches through public sources. The TIBER-EU Scope Specification can be a basis for this.
- TI providers should use a broad range of sources (e.g. internet services, a mixture of public and private fora and a range of media types such as internet relay chats, email and video). The number of items in any given source type is again a useful means of measuring the likely catchment capability of any collection function.

However, the volume can at times undermine ability, it is expected that the collection off sources is balanced against the ability of the TIP to refine, analyse and discard sources in an accurate manner. This all results in a weighted analysis.
- Cyber security service providers should have adequate language support. Languages play an important role in providing cyber threat intelligence. Cyber threats are a global phenomenon, and a TIP that offers little linguistic coverage of online threats will potentially miss a significant proportion of relevant information.
- TI providers should be able to use a variety of methods in intelligence gathering, for example OSINT (which is derived overtly from publicly available sources).
- TI providers must always demonstrate strong ethical behaviour.
- TIP and RTP must work together in a collaborative, transparent and flexible manner. A TIP must demonstrate willingness and the ability to work in this way, sharing its deliverables with its RTP counterpart for review and comment. The TIP should also demonstrate a willingness to work with the RTP during the remainder of the test. This includes the creation of testing scenarios, as well as any new intelligence requirements that occur as the test progresses. The TIP is expected to provide input into the final report issued to the FI.
- Should the TIP and the RTP be separate parties, it is essential that the RTP is involved during the TI phase.

When the TTI Report is finished there is a formal handover from the TIP to the RTP.

5.3 Test Plan

In the Test Plan, the RTP will put together scenarios for the TIBER-NL test which:
- Combine the Generic Threat Landscape Report (TCT) and Target Threat Intelligence Report (FI + RTP/TIP) and aligns these into credible scenarios;
- Map onto one or more Critical Function supporting systems;
- Provides background to the tradecraft of the type of threat actor that is mimicked in the test;
- Provides creative elements of what Tactics, Techniques and Procedures 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 impact 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.

<u>Attack scenarios</u>
Scenarios should be built based on the TIBER-NL Generic Threat Landscape Report, the TIBER-EU Scope Specification document, the TTI Report and targeting information and high level scenarios of the previous sections.
The scenarios are written from the threat actors' point of view and are intelligence-led. The RTP indicates various creative options in each of the test phases based on various tactics, techniques and procedures used by advanced threat actors, to anticipate changing circumstances or if the first option does not work. The RTP should also indicate where a leg up might be needed if the attack is not successful. 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. In the attack scenario's leg ups should be defined in case a RTP cannot complete one of the phases.

In addition to these scenarios, a scenario X is prepared. This scenario enables a forward-looking perspective to the attacks. The goal of scenario X is to look forward towards what advanced attacks can be expected in the (near) future. This scenario can be focused around a certain innovative technique, on tactics the RTP and TIP sees developing possibly combined with societal developments that will impact FI in the coming future. The end goal of Scenario X is still a CF, the way towards the CF allows for a large level of creativity. Scenario X will be decided upon by the WT and TTM, supported by the RTP and TIP, during week six has passed.

Rules of engagement
Part of the test plan should be the rules of engagement. This is a part of the test plan where the RTP lays down the rules they will abide to during the engagement. The rules of engagement should contain at least the following:

- High level description of the techniques being used during the attack;
- List of excluded techniques;
- Detailed description of scenario's used for social engineering;
- How privacy of both voluntarily and involuntarily participants is being safeguarded in compliance with rules & regulations.

Detailed out phase plan
Before the start of the out phase a plan has to be delivered by the RTP on how they will approach the out phase. This plan should contain at least the following elements:

- Detailed description of the objective on the out phase and the scope of the out phase;
- Detailed description of the TTP's being used during the out phase;
- An overview of business knowledge needed to perform the out phase;
- A list of possible specialists needed to perform the out phase;
- Risks to be managed during the execution of the out phase.

It's up to the WT to supply the asked business knowledge and the specialists. The TIP has to judge whether the asked knowledge is realistic in comparison to the simulated threat actor. If it's not deemed realistic it is advisable that the WT makes a judgment call on whether to supply the information or not. This depends on the risk for the continuity of the business of the proposed actions.

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 cyber security service providers must observe, such as the time and resources available – not to mention the moral, ethical and legal boundaries.[1] 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 CF's 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 threat actors with the capacity and time to study these extensively.

Therefore, it depends on the entity 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

1 It is up to the entity 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.

relevant information an FI gives to the RTP the more the FI 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 threat actors could not have gotten that information. Therefore it should be evident that the information given to the RTP could have been obtained by an advanced threat actor, given more time, different known techniques etc. Whether this information is provided by the FI or delivered by a TIP, is up to the FI.

Figure 5.2 Balancing information entity and TIP/RTP

The above figure 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 TTM decides, on the basis of the FI's request, if an extra GIA check is necessary.

<u>Approval of the attack plan</u>
At three points during the test there will be a formal approval of the attack plan:

- Before the test phase starts the attack plan is approved by the WT, TTM, TIP and RTP;
- After six weeks when scenario X is finalized the attack plan will be approved by the WT, TTM, TIP and RTP;
- After eight weeks the attack plan is finalized and approved again when the detailed plan for the out phase is added.

5.4 Test

The Test Plan also provides a planning for the execution of the test. The timespan for actual testing should be at least twelve weeks. Please note that for this reason there can be a difference between actual working time in weeks (for example six) and test weeks in the planning (ten to twelve), in order for the RTP to be able to work in a stealthy manner and e.g. pause when needed after detection.

The RTP now moves into execution of the TIBER test during which it performs a stealthy intelligence-led red teaming exercise on the target systems. 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 threat actors would) to develop alternative ways to reach the test objective. This is always done in close contact with the WT and the TTM. All actions of the RTP are logged for replay with the BT, evidence for the RTP 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 WT and the overall aim is to improve the BT 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).

RTP 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 WT 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 WT and with the TTM. The TTM is updated at least once a week by the RTP and WT on the progress. Physical meetings between the WT, TTM and RTP during this phase are strongly encouraged since the discussions add significantly to the quality of the test. Also, FI have had very positive experiences when a member of the WT is onsite with the RTP for some time during the engagement.

During week six of the test there is a cut-off point. If after 6 weeks the red team has not been able to complete the “in phase” the RTP will be provided with a realistic leg up so the rest of the scenario can be played or, in case the RTP has gained foothold in another scenario it can be allowed to use that path for the rest of the scenario where the “in phase” failed.

Removing the TIBER-NL label of a test

As the TCT is not part of the commercial negotiations between the RTP and the FI it cannot stop the test. It however has the power to remove the TIBER-NL label. Which means the test isn’t recognized as a TIBER-NL test. This means that, in case this was a multi-jurisdiction test, the test won’t get the recognition of a TIBER-XX test in other jurisdictions. The TCT should therefore be very careful in its decision to remove the TIBER-NL label.

The TCT can remove the TIBER-NL label in the following situations (this is not an exhaustive list. The decision will always be made in consultation with the WT unless the situation doesn’t permit this):

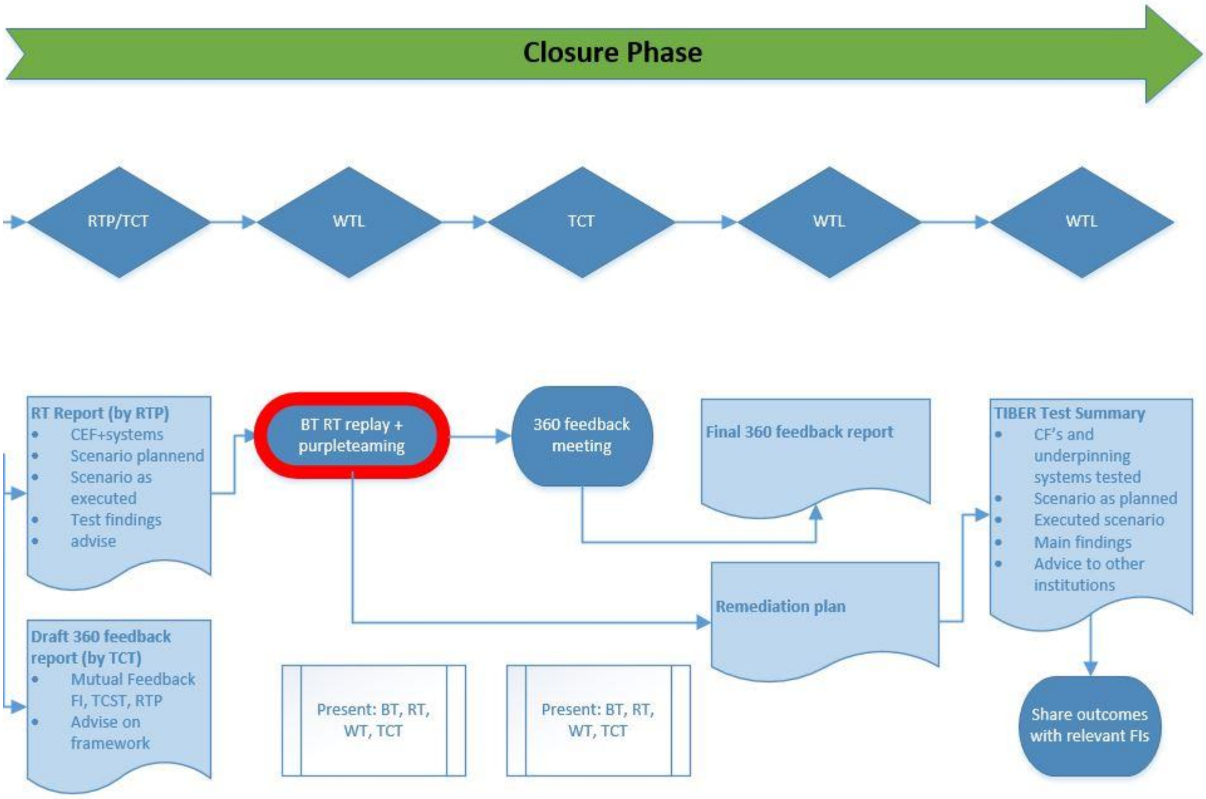
- Either the TIP or the RTP has repeatedly shown it cannot live up to the standards laid out in the TIBER-NL framework;
- The test has been compromised by the RTP, TIP or the FI either intentional or as a result of gross negligence;
- When there is foul play by the BT;
- All other situations which compromise the quality or the secrecy of the test.

Should the TCT decide to remove the TIBER-NL label the FI can choose to continue with the test gaining the learnings from the test but without it being recognized as a TIBER-NL test, or the FI can consult with the TCT what steps have to be undertaken to make the test a TIBER-NL recognized test (again).

6. Closure & Learning Phase

6.1 Overview
The duration of the activities in this final phase of work is approximately four weeks.

Figure 6.1 Closure & Learning Phase



<u>Relevant documentation</u>
- format Red Team Test Report;
- format TIBER-NL Test Summary;
- format 360 Feedback Report.

<u>Outputs</u>
- Red Team Test Report;
- Blue Team Report;
- Remediation Report;
- TIBER-NL Test Summary;
- Information shared with other FI on test outcomes;
- 360 feedback report.
-

6.2 Red Team Test Report and Blue Team Report
The output of this activity is a draft version of the Red Team Test Report produced by the RTP for delivery to the FI. The draft report must be issued within two weeks of test completion. The report must give an overview of the whole TIBER-NL process, including the CFs in scope, the threat intelligence base of the test, the scenarios planned, the scenarios executed, the findings of the test and the advice of the RTP to the FI. The key members of the FI's BT are informed of the test and will use the Red Team Test Report to deliver their own BT report. In the BT report, the BT maps its actions alongside the RTP actions. The BT report should be completed ahead of the purple teaming workshop (see

Section 6.3 below) to maximise the learnings from the replay. Should the BT have no idea of the test or not enough information for a BT report the RTP should provide IOC's to the BT to help them with the BT report.

6.3 Purple teaming

After the RTP delivers its report, the FI arranges a purple teaming workshop. This workshop lasts at least a full day. Often this phase is perceived as the most educational and hence more days are being used. The goal of this workshop is to enhance the learning experience. During the purple teaming workshop the RTP and FI should replay the attack and collaborate with each other to enhance specifically the defensive capabilities of the FI, as a spin off the attacking capabilities of the RTP will grow. The TTM should be present during parts this meeting. Purple teaming and who should be involved and participate will be described in more detail in the TIBER purple teaming guide. Purple teaming in TIBER-NL is an expansion of the replay where the learning experience for both the BT and the RTP is enhanced.

6.4 360 feedback

During the 360 feedback meeting, the FI (WT and BT), TCT, TIP and RTP will come together to review the TIBER-NL exercise. The TTM 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 RTP, 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.

6.5 Remediation plan and TIBER-NL Test Summary

Based on the test outcomes the FI should 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. Input for the remediation plan can be the TIP report, the RTP report, the BT report, input from the WT and organisational findings.

The TIBER-NL Test Summary summarises the TIBER-NL process and should draw upon the delivered documentation such as the RTP and BT reports, the generic threat actor intelligence, the targeted threat intelligence and when available its remediation plan(s).

The gathered intelligence and lessons learned from the test will be input for the Generic Threat Intelligence Report used in future tests.

6.6 Metrics

Metrics are being developed for the TIBER-NL framework. Aim is to work on an objectification of the tested FI's security posture relative to the emulated level of attack. In several tests the TCT, TIP and RTP will forge the results of the tests into various sets of metrics, at the moment of writing as a pilot. When the pilot proves successful, in a later version of the framework the metrics will be added and described in detail.

6.7 Result sharing

1. Board level executives

It is of the utmost importance that the board level of FI is informed on threats, test results and the remediation plan (risk mitigation measures). The TCT will be attending the presentation of the results and findings to board level and the TCT will stress the importance of board attention, support and accountability in executing the remediation plan.

2. White Team Leads
Since the TIBER-NL test focuses on the Dutch financial sector as a group, sharing of information between the FI is in important part of the TIBER-NL framework. As one of the main goals of TIBER is enhancing the sector's operational resilience against advanced threat actors, the FI shares effective remediation solutions and best practices 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 TCT and the WT can discuss the forum for sharing the information, and the level of detail. In general, results are shared during the WTL meetings in which the White Team Leads of the different FI.

3. Oversight and / or supervisor
The TCT 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 TCT will notify the supervisor and / or overseer that the test has ended and informs them in general terms about the TIBER process, its goals and way of working. The FI informs its supervisor and / or overseer about the test. The RTP test report and other sensitive documents belonging related to the TIBER-NL process will remain on premise of the FI. The TCT can be invited to give an explanation regarding the TIBER-NL program and the level of testing during this meeting.

7. Annex I: Abbreviations used in this document

Term	Explanation
BT	Blue Team
CBEST	The Bank of England cyber resilience program on which TIBER-NL is based
CF	Critical Functions
DNB	Dutch Central Bank (De Nederlandsche Bank)
FCI	Financial Core Infrastructure
FI	Financial Institution(s)
ECB	European Central Bank
GIA	Governmental Intelligence Agency
GTL	Generic Threat Landscape
MO	Modus Operandi
NCSC	Nationaal Cyber Security Center
NDA	Non-Disclosure Agreement
IOC	Indicators of Compromise
OSINT	Open Source Intelligence
RT	Red Team
RTP	Red Teaming Provider
TCT	TIBER(-NL) Cyber Team
TECHINT	Technical Intelligence
TI	Threat Intelligence
TIA	Threat Intelligence Advisor
TIP	Threat Intelligence Provider
TIBER	Threat Intelligence Based Ethical Red teaming
TTI	Targeted Threat Intelligence
TTP	Tactics, Techniques and Procedures used in a cyber attack
TTM	TIBER(-NL) 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 that have been aligned with the TIBER-EU documentation. 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

- TIBER-EU White Team Guidance
- TIBER-EU Services Procurement Guidelines
- TIBER-EU White Team Guidance
- TIBER-EU Scope Specification document
- Generic Threat Intelligence Report

Test Phase

- Format Targeted Threat Intelligence Report
- Format Test Plan

Closure Phase

- Format Red Team Test Report
- TIBER-EU Format 360 Feedback Report
- Format TIBER-NL Test Summary
- Purple team guide (awaiting publication at the moment of writing)