TIBER-NO Operational Guide

Version 1.3

11 June 2024

Contents

1 Introduction

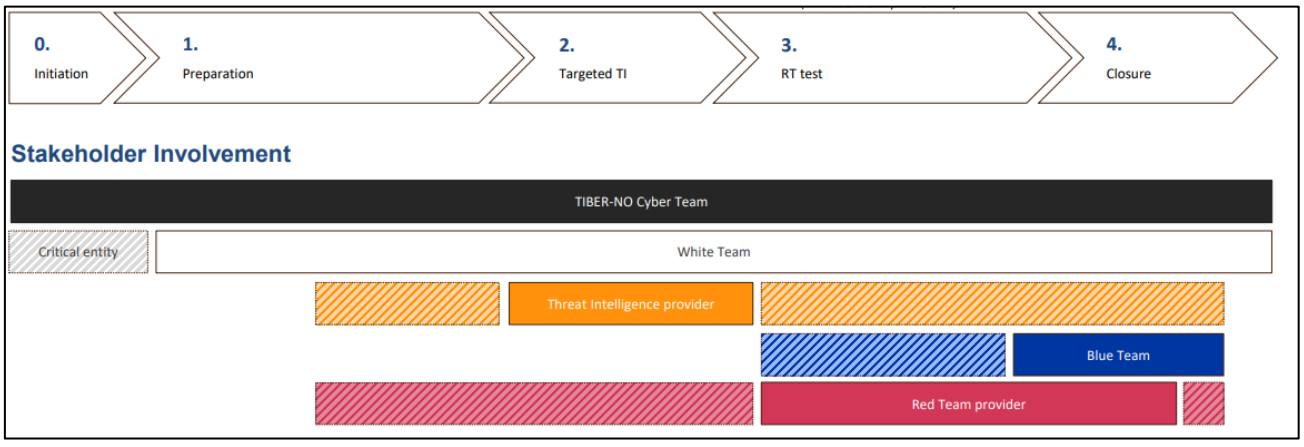
TIBER-EU is a European framework for intelligence-based ethical red team testing developed by the European Central Bank. TIBER-NO is the Norwegian implementation, based on and harmonized with the requirements from the framework. TIBER-EU delivers a controlled, bespoke, threat intelligence-led red team test process for entities' critical live production systems. The TIBER-NO implementation is governed and maintained by Norges Bank and Finanstilsynet (The Norwegian Financial Authority). TIBER-NO testing is intended for entities responsible for critical functions in the Norwegian financial sector. The aim of TIBER-NO is to strengthen cyber-resilience and contribute to the stability of the Norwegian financial system.

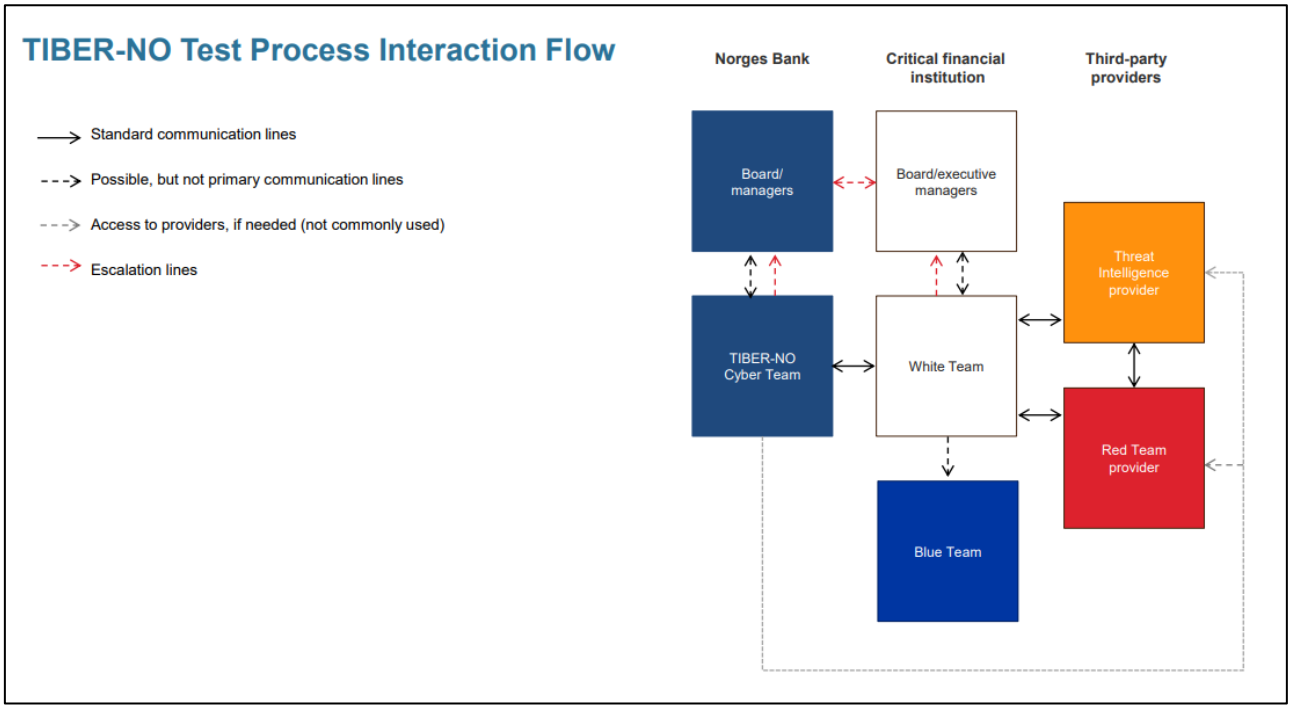
The TIBER Cyber Team at Norges Bank would like to thank the team at Nationalbanken in Denmark for the great support in establishing TIBER in Norway. This TIBER-NO Operational Guide and accompanying documents are based on similar documentation for TIBER-DK.

1.1 The purpose of this guide

This guide, the TIBER-NO Operational Guide, provides a step-by-step description of each of the elements in the TIBER-NO test process. The TIBER-NO Implementation Guide describes how the requirements in TIBER-EU are adopted and implemented in a Norwegian context, including roles and responsibilities for the stakeholders involved in a TIBER-NO test. This Operational Guide refers to documents common to all jurisdictions that have adopted TIBER-EU and documents specific for TIBER-NO.

1.2 TIBER-NO test process overview





1.3 Abbreviations

The following abbreviations are used in the TIBER-NO documents:

TCT	TIBER-NO Cyber Team at Norges Bank
WT	White Team
RT	Red Team
BT	Blue Team
TI	Threat Intelligence
TTP	Tactics, Techniques and Procedures
OSINT	Open-Source Intelligence

1.4 Preconditions

TIBER-NO is a voluntary security testing programme for entities critical to the Norwegian financial system. The TIBER-NO programme is owned by Norges Bank and Finanstilsynet and managed and operated by the TIBER Cyber Team, TCT, at Norges Bank. Before a TIBER-NO test process can be initiated, the following preconditions must be met:

- The entity has agreed to participate in the TIBER-NO programme.
- Norges Bank has deemed the entity eligible for the TIBER-NO programme based on its role in the Norwegian financial system.

The TCT will make sure the entity has access to all material relevant for the planning of the TIBER-NO test.

As TIBER-NO is not a regulatory requirement, participation is voluntary. Together Norges Bank and Finanstilsynet is the lead authority of TIBER-NO and thus responsible for overseeing each TIBER-NO test to ensure the test meets the requirements in the TIBER framework and can be recognised as a TIBER test. This requires that the TCT can review and approve all the relevant material prepared in the test process. The TCT will not share information about a TIBER test with any other authority without having clear consent from the tested entity. The only exemption is the TCT can share anonymised and aggregated information with the TIBER collective.

The tested entity is the legal owner of all material produced during the test and responsible for sharing the material with its competent authorities if required. When testing cross-border entities participating in TIBER-NO, the TCT can upon request enter cooperation with authorities in other jurisdictions. Such cooperation requires a specific consent from the tested entity and must be entered in accordance with the conditions described in this section.

There may be other preconditions required at an early stage for a successful TIBER-NO test, and these are often individual for each test entity. These could be, for instance, internal considerations about legal and contractual agreements as well as budgeting and resource allocation for the project. An early dialogue with the TCT can be arranged to discuss the test scope and test process to allow the entity to appropriately estimate the size and the costs of the project.

1.5 Documents

The TIBER-NO implementation consists of a series of documents. Some contain mandatory requirements for TIBER-NO testing, while others are guidance documents or templates.

The latest version of documents can be obtained from:

- TIBER-EU: https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html
- TIBER-NO: https://www.norges-bank.no/tiber
- Contacting TCT directly for non-published documents

TIBER-EU documents:

- TIBER-EU Framework
- TIBER-EU White Team Guidance
- TIBER-EU Scope Specification Template
- TIBER-EU Services Procurement Guidelines
- TIBER-EU Guidance for Target Threat Intelligence Report
- TIBER-EU Guidance for the Red Team Test Plan
- TIBER-EU Guidance for the Red Team Test Report

- TIBER-EU Purple Teaming Best Practices
- TIBER-EU Guidance for the Test Summary Report
- TIBER-EU Attestation Template

TIBER-NO documents:

- TIBER-NO General Implementation Guide / TIBER-NO Implementasjonsveiledning
- TIBER-NO Operational Guide (this document)
- TIBER-NO Generic Threat Landscape Report (NFCERT)
- TIBER-NO Risk Management Guidance
- TIBER-NO Leg-up Guidance
- TIBER-NO Targeted Threat Intelligence Report Guidance
- TIBER-NO Red Team Test Plan Guidance
- TIBER-NO Blue Team Test Report Guidance

Templates to be filled out:

- TIBER-NO Test Overview (Excel)
- TIBER-NO Non-Disclosure Agreement (optional)
- TIBER-NO WT and TCT Rules of Engagement
- TIBER-NO Scope Specification Template. Based on the TIBER-EU Scope Specification Template
- TIBER-NO Letter of Attestation for Scope
- TIBER-NO Letter of Attestation for Scope – Service Provider
- TIBER-NO Red Team Status Reporting (PowerPoint)
- TIBER-NO 360º Feedback Report

Additional documents created by the Entity:

- Detailed Project Plan
- Scope Specification
- Theat Intelligence Provider Contract
- Red Team Provider Contract
- Risk Management Documentation
- Blue Team Test Report (Entity's own use)
- Remediation Plan (Entity's own use)
- Test Summary Report

Documents created by Threat Intelligence Provider:

- Targeted TI Report

Documents created by Red-Team Provider:

- Red Team Test Plan
- Red Team Test Report

Other supporting documents:

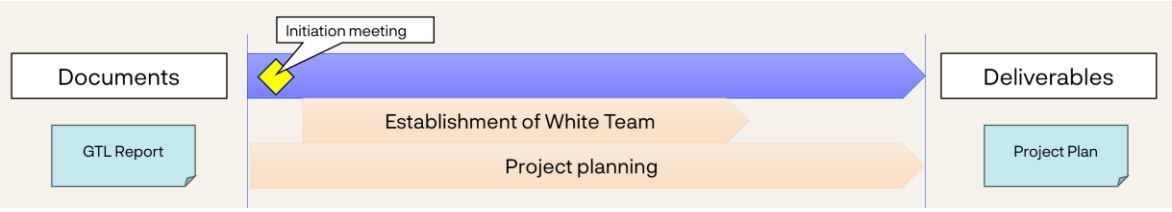
- TIBER-NO Scope and Scoping Workshop - Supporting Document

2 Initiation phase

During the Initiation phase the entity should get acquainted with the requirements in the TIBER-NO General Implementation Guide and consider which arrangements need to be made before the test can be launched. This can be achieved by reading the following documents:

- TIBER-NO General Implementation Guide
- TIBER-NO Operational Guide
- TIBER-NO Test Overview (Excel)
- TIBER-EU White Team Guidance
- TIBER-EU Services Procurement Guidelines

The Initiation phase involves several key activities to get the project up and running. Activities from the following Preparation phase can also be started tocreate the basis for a successful TIBER-NO test.



2.1 Establishment of White Team [Activity]

- Responsible: Entity
- Deliverables:
  - TIBER-NO Test Overview (Excel) (White Team members)
  - TIBER-NO WT and TCT Rules of Engagement
  - TIBER-NO Non-Disclosure Agreement (optional)
- Documents:
  - TIBER-EU White Team Guidance
  - TIBER-NO WT and TCT Rules of Engagement
  - TIBER-NO Non-Disclosure Agreement

As part of the Initiation phase the entity must establish the White Team (WT), which is the management group for the TIBER-NO test. The entity must follow the TIBER-EU White Team Guidance to establish a WT with a dedicated WT lead. Since the WT lead coordinates all test preparations and test activities, including coordination of the TI and RT providers and meetings with the TCT, the WT lead should be appointed early in the Initiation phase.

Due to the importance of the White Team Lead role, at least one other member of the White Team should be kept well informed about all details to stand in for the White Team Lead if needed.

The WT lead is foreseen to use a substantial amount of time during all phases of the TIBER-NO test and is expected to be a senior resource with great project management and communication skills.

The WT should conduct an initial stakeholder analysis to consider which stakeholders besides the TCT and the TI and RT providers need to be involved in the WT, such as critical service providers or data centres.

Once the WT is established the WT lead will inform the TCT of its members by adding the names and contact information to the document TIBER-NO Test Overview (Excel). The WT can be supplemented as the preparations continue. The WT can be further extended, for instance to include key personnel from critical suppliers.

Due to the sensitive nature of the preparation and execution of the TIBER-NO test, the entity should consider the need for WT members to sign a non-disclosure agreement (NDA) to ensure internal and external confidentiality of the test.

2.2 Project Planning [Activity]

- **Responsible**: Entity
- **Deliverable**
  - Detailed Project Plan
    - Deadline: One week prior to the Launch meeting [Meeting]
- **Document**
  - TIBER-NO Test Overview (Excel) (optional)

The first steps towards a Detailed Project Plan are taken in the Initiation phase and the activity carries over into the Preparation phase.

In the Initiation phase the entity should plan the allocation of the right resources to the WT, and in the beginning of the Preparation phase the WT lead should start drafting a Detailed Project Plan. The entity may use its own format for the Detailed Project Plan. The content of the plan can be based on the plan found in the TIBER-NO Test Overview (Excel) and the dates agreed upon by the entity and the TCT. The Detailed Project Plan must include a schedule of meetings to be held between the WT, the TI provider, the RT provider and the TCT to review deliverables.

The Detailed Project Plan must be finalised by the end of the procurement process (Preparation phase) and is to be shared with all stakeholders in advance of the Launch meeting [Meeting]. Though finalised, the entity can still make minor adjustments and continuously update the project plan given that changes are discussed in advance with the TCT.

2.3 Initiation meeting [Meeting]

- **Responsible**: TCT
- **Participants**: TCT, Entity
- **Preparation**:

        - TIBER-NO Test Overview (Excel), responsible: TCT
            - Deadline: One week prior to the Initiation meeting
- **Meeting outcomes**:
    - Agree on a launch date.
    - Choose a code name for the entity.

Each TIBER-NO engagement starts with an Initiation meeting for which the TCT is responsible. The main outcome of the meeting is for the entity and the TCT to agree on a date for the launch of the test. The launch date should be set well in advance and leave an appropriate amount of time for preparation of the test, including time for the entity to allocate the proper resources for the TIBER-NO test in its budgeting. Furthermore, the launch date should be set to fit the TCT's plan for other tests in the TIBER-NO programme.

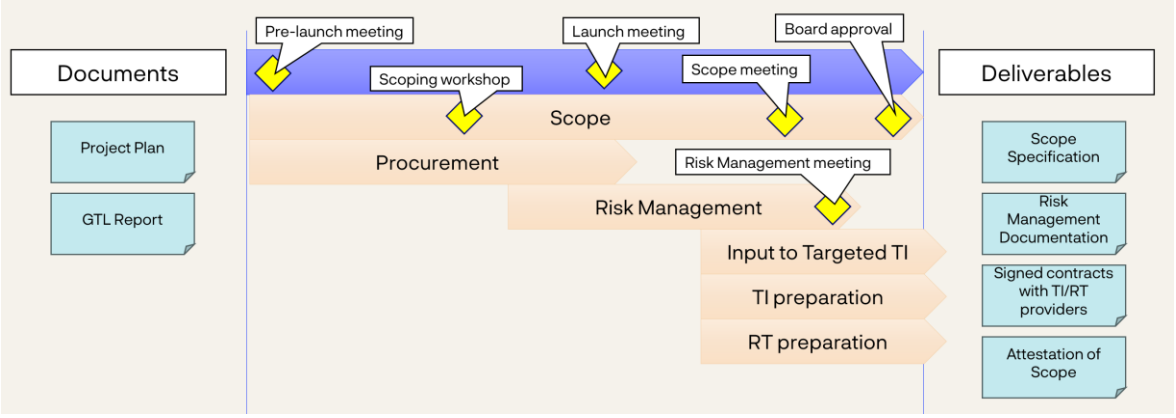
The TCT will provide a suggestion for dates in a TIBER-NO Test Overview (Excel), including a suggested launch date, to the entity prior to the Initiation meeting. This overview and the launch date will be discussed at the Initiation meeting.

To protect the sensitive nature of the test, a code name for the entity should be chosen at the Initiation meeting (see below on risk management practices). This code name will be used by all stakeholders when referring to the entity throughout the remainder of the test process.

At the Initiation meeting, the TCT will introduce the entity to the requirements and documentation for a TIBER-NO test for the Initiation and Preparation phases. The main topics are ***Error! Reference source not found.***, *Project Planning [Activity]*, *Scoping [Activity]* and *Procurement [Activity]*.

3 Preparation phase

The Preparation phase contains activities key to a successful TIBER-NO test. Activities started in the Initiation phase are expected to intensify in the Preparation phase. To ensure the preparations progress according to plan, regular status meetings between the WT and the TCT are scheduled at the Pre-launch meeting [Meeting].



3.1 Scoping [Activity]

- **Responsible**: WT
- **Deliverables**:
  - Scope Specification
    - Deadline: One week prior to the Scope meeting [Meeting]
  - TIBER-NO Letter of Attestation for Scope
    - Deadline: Immediately after the Scope meeting [Meeting]
  - TIBER-NO Letter of Attestation for Scope – Service Provider
    - Deadline: (If applicable) Immediately after the Scope meeting [Meeting]
- **Documents**:
  - TIBER-EU Scope Specification Template
  - TIBER-NO Scope Specification Template
  - TIBER-NO Letter of Attestation for Scope
  - TIBER-NO Letter of Attestation for Scope – Service Provider

The test scope defines important boundaries to help the WT focus its efforts and is useful in several processes and activities throughout the TIBER-NO test. The entity should consider its Critical Functions and supporting systems at an early stage, as initial steps towards the creation of a test scope.

The key objective of the scoping is for the entity and the TCT to agree on the scope of the red team test. The scope must include the entity's critical functions. The entity may decide to include additional non-critical functions (such as roles, processes, and technologies) in the scope of the test, provided these do not negatively affect the testing of the critical functions.

TIBER-EU Framework defines in chapter 7.5 Critical Functions as "the roles, processes and technologies required by the entity to deliver a core service which, if disrupted, could have a detrimental impact on financial stability, the entity's safety and soundness, the entity's customer base or the entity's market conduct".

To ensure the test runs effectively, the relevant stakeholders of the test should be considered, including the role of service providers critical for the delivery of core services to the entity.

During the scoping process, the entity must complete the TIBER-NO Scope Specification Template resulting in the Scope Specification. This document sets out the scope of the TIBER-NO test and lists the key systems and services that underpin each critical function. This information helps the WT set the 'flags' to be captured, which are essentially the targets and objectives the RT providers will strive to achieve during the red team test.

The WT should discuss the flags with the TCT, who must approve them. Although the flags are set during the scoping process, they may be changed in later phases such as following the threat intelligence gathering and as the Red Team test evolves.

To ensure a good and timely scoping process, the TCT initiates the discussion of the test scope as early as in the Initiation meeting and will facilitate a Scoping workshop [Meeting] early in the Preparation phase. From there, the WT and TCT will be in an ongoing dialogue regarding the scope until the finalisation of the Scope Specification at the Scope meeting [Meeting]. Importantly, the scope will need to be agreed and attested by the board of the entity. If a service provider is directly involved in the test, the inclusion of its critical systems into the entity's test scope should also be attested by the board/executive management of the service provider.

3.2 Procurement [Activity]

- **Responsible**: WT
- **Deliverables**:
    - Signed Theat Intelligence Provider Contract and Red Team Provider Contract
        - Deadline: One week prior to the Launch meeting [Meeting]
- **Documents**:
    - TIBER-EU Services Procurement Guidelines

The time needed for procurement differs across entities. The procurement process for external TI and RT providers should be started early, often already in the Initiation phase, to allow for this.

Although some entities may already conduct red team testing with dedicated internal red teams, the TCT will only recognise a TIBER test if testing is conducted by independent third-party providers (external TI and RT providers). Employees of the entity’s internal red team may of course contribute to White Team tasks apart from the testing performed by the external providers.

To ensure the TI and RT providers meet the appropriate standards for conducting such a test, the entity should consider the guidance and minimum requirements set out in detail in the TIBER-EU Services Procurement Guidelines. Furthermore, it is the responsibility of the entity, the TI provider and the RT provider to ensure they conduct tests within the remit of all laws and regulations and appropriate risk management controls (such as contracts) are in place to enforce this.

TI and RT providers with adequate experiences are key means of managing the risks associated with the TIBER-NO test, and the WT must use competent, qualified, and skilled TI and RT providers to meet the expected high standards of risk management.

When procuring TI and RT providers, the WT should make sure there is a 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). Review steps, logging, physical presence at meetings (preferred at mandatory meetings) and report examples can be taken into consideration. The contracts with the TI and RT providers should include:

- the providers must meet security and confidentiality requirements at least as stringent as those followed by the underlying entity.
- protection of those involved (e.g. indemnifications)
- a clause related to data destruction requirements and breach notification provisions.
- a determination of activities not allowed during the test, such as: destruction of equipment; uncontrolled modification of data/programs; jeopardising the continuity of critical services; blackmail; threatening or bribing employees; and disclosure of results.

Signed contracts with the TI provider and the RT provider should be in place at the latest one week prior to the Launch meeting [Meeting]. The contracts should not be shared with the TCT.

Once the procurement process has been completed, all relevant contractual arrangements should be in place.

3.3 Risk Management [Activity]

- **Responsible**: WT
- **Deliverable**:
    - Risk Management Documentation
        - Deadline: One week prior to the Risk management meeting
- **Documents**:
    - TIBER-NO Risk Management Guidance

The TIBER-NO test includes elements of risk owing to the criticality of the target systems as well as the roles and the processes involved in the tests. The WT is responsible for implementing appropriate controls, processes, and procedures to ensure the test is

carried out with sufficient assurances for all stakeholders, and that risks will be identified, analysed and mitigated according to the entity's practices regarding risk management. This includes:

- A risk assessment should be conducted prior to the test to make sure the right risk management precautions are taken in line with the entity's existing risk management framework.
- Protecting the confidentiality of the test is crucial to its effectiveness, and the WT should limit awareness of the test to a small, trusted group whose members have the appropriate levels of seniority to make risk-based decisions regarding the test.
- Due diligence of in-scope systems prior to any testing should be part of the preparations to ensure backup and restoration capabilities are in place. This should be carefully carried out such that the in-scope systems are not revealed to employees outside of the WT.
- A code name for the entity should be used by all stakeholders throughout the whole process to protect the sensitive nature of the test and the potentially detailed findings on the weaknesses and vulnerabilities.
- Escalation procedures should be documented and monitored by the WT to enable the WT to prevent the BT from taking any actions that would be appropriate in case of a real event but could impact the entity's operations. Such actions include, but are not limited to, shutting down systems and contacting police, security authorities or other relevant authorities, e.g., data protection authorities.
- The management of risks during the test requires the WT to remain in control of the process to ensure the test proceeds according to agreed-upon scope, timeline and scenarios and the process described in the framework documents.
- If physical security is included in the test scenario, appropriate safeguards should be in place (such as a 'get out of jail' letter). The entity should consider analysing any legal, ethical, or other issues in advance of the launch of the test.

The WT should document to the TCT that appropriate risk management activities have been conducted prior to the Risk management meeting. For this, the Risk Management Documentation should be produced by the WT at the latest one week prior to the Risk management meeting [Meeting]. See the TIBER-NO Risk Management Guidance for a suggested format and ideas for risks and mitigating actions.

Finanstilsynet (The Norwegian Financial Supervisory Authority) requests entities conducting TIBER-NO tests to notify them of the period of active testing in advance to reduce the impact if they inadvertently should be contacted related to the testing. This is voluntary. Notifications can be sent to Tiber_test@finanstilsynet.no, preferably with “Tiber-test” in the subject line.

3.4 Input to Targeted TI [Activity]

- **Responsible**: WT
- **Deliverables to TI provider**:
    - TIBER-NO Generic Threat Landscape Report

        - Deadline: Start of Targeted TI phase
    - Scope Specification
        - Deadline: Start of Targeted TI phase
- **Document**:
    - TIBER-EU Guidance for Target Threat Intelligence Report
    - TIBER-NO Targeted Threat Intelligence Report Guidance

The TIBER process is designed to create realistic threat scenarios describing attacks against an entity's critical functions. Real-world threat actors may have months to prepare an attack. Hence, to make intelligence gathering as efficient as possible given the time and resource constraints, the TI provider should seek from the WT and be provided with relevant information that might help their analysis. Some examples of the information that should be provided are:

- a business and technical overview of each critical function-supporting system in the scope
- the current threat assessment and/or threat register
- examples of recent attacks.

Obtaining the relevant input for the TI provider without alerting the organisation of an imminent test may require the WT to gather information slowly and to use convincing cover stories. This activity may begin as early as the Preparation phase once the contract with the TI provider is signed.

Ensuring a controlled information flow towards the TI provider is imperative. The information given by the WT to the TI provider should serve to help focus their analysis. The information contained in the Targeted TI Report should be confirmed by the TI provider through other sources.

3.5 TI Preparation [Activity]

- **Responsible**: TI provider

The TI provider should start preparations for the Targeted TI phase, for instance agreeing on a detailed time schedule for the Targeted TI phase in line with the Detailed Project Plan. If relevant, the TI provider should give input to the scope and risk management.

3.6 RT Preparation [Activity]

- **Responsible**: RT provider

The RT provider should start preparations for the RT Test phase, for instance agreeing on a detailed time schedule for the RT Test phase in line with the Detailed Project Plan. If relevant, the RT provider should give input to the scope and risk management, for instance regarding rules of engagement.

3.7 Pre-launch meeting [Meeting]

- **Responsible**: TCT

- **Participants**: WT, TCT
- **Preparation**:
    - TIBER-NO Test Overview (Excel), responsible: TCT
    - Appoint WT Lead, responsible: Entity
    - Establish WT, responsible: Entity
    - Draft TIBER-NO WT and TCT Rules of Engagement, responsible: WT, TCT
- **Meeting outcomes**:
    - Finalise Detailed Project Plan
    - Schedule regular status meetings, responsible: TCT
    - TIBER-NO WT and TCT Rules of Engagement, responsible: WT, TCT

At least three months before the agreed launch date, the TCT will invite the WT to a Pre-launch meeting. This meeting marks the start of the planned and agreed-upon TIBER-NO test process for each individual entity.

At the Pre-launch meeting, the entity and the TCT will agree on the Detailed Project Plan.

The TCT will make sure the WT is well-acquainted with the requirements of the TIBER-NO test process. The WT can raise any concerns that have been identified during the initial project planning Discussions on scope and procurement will be initiated.

Finally, regular status meetings between the WT and the TCT are agreed. At these status meetings, the progress of the test preparations will be discussed, and the TCT can provide guidance to the WT. Status meetings shall be held approximately every fortnight in the preparation phase and may be supplemented with additional meetings. In the Targeted TI phase, the Red Team test phase and the Closure phase, the status meetings will be arranged as needed and as a supplement to TI and RT meetings and other meetings arranged by the WT lead. The meeting frequency in all phases can be changed if all parties agree.

The generic agenda for the status meetings is:

1. Overall status from White Team
2. Overall status from TCT
3. Detailed status on ongoing activities in the plan, including coordination
4. Start of new activities in the plan, including coordination
5. Follow up on progress
6. Other issues

3.8 Scoping workshop [Meeting]

- **Responsible**: TCT
- **Participants**: WT, TCT
- **Preparation**:
    - Create a gross list of critical functions, responsible: WT
    - Acquire information on high-level system architecture, responsible: WT

- Acquire information on critical business processes, responsible: WT
- **Meeting outcome**:
  - Identification of the entity's critical functions, its underpinning critical systems, processes and potential flags

To ensure a good start of the scoping activity, the TCT will arrange one or more Scoping workshop [Meeting] dedicated to the discussion of the TIBER-NO test scope.

In preparation for the Scoping workshops, the WT lead should create a gross list of the entity's critical (business) functions and investigate how they depend on critical IT systems, roles and processes. For this purpose, for example high-level system architecture diagrams or the like should be acquired to provide an overview of the entity's critical systems underpinning the critical functions.

At the Scoping workshop, the WT will present the critical functions and explain the high-level system landscape of the entity to the TCT. For this purpose, it may be relevant to include subject matter experts with extensive insights into both the business and IT side of the entity, taking into consideration the confidentiality of the test. If these resources are not already present within the WT and if the entity chooses to include them, the subject matter experts could sign an NDA.

The outcome of the Scoping workshop is to identify the entity's critical functions, its underpinning key systems, processes, and potential flags.

3.9 Launch meeting [Meeting]

- **Responsible**: WT
- **Participants**: WT, TCT, TI provider, RT provider
- **Preparation**:
  - Detailed Project Plan, responsible: WT
    - Deadline: One week prior to the Launch meeting
  - Presentation of TI team and methodology, responsible: TI provider
  - Presentation of RT team and methodology, responsible: RT provider
- **Meeting outcomes**:
  - Agree on the Detailed Project Plan
  - Establish a good basis for collaboration.
  - Align expectations.

The Launch meeting should involve all relevant stakeholders, including the TCT, the WT, the TI provider, and the RT provider. In case of logistical restraints, remote participation can be arranged, but physical representation is strongly encouraged. During this meeting, all stakeholders discuss the test process, their cooperation and roles during the test process and their expectations of the test process as well as the Detailed Project Plan. The plan is prepared and delivered at the latest one week prior to the Launch meeting by the WT (*Project Planning [Activity]*).

At the meeting, the TI provider and the RT provider are expected to present their teams and explain their methodology regarding the TIBER-NO assignment and the entity's test scope. The TI provider and the RT provider should outline how they expect to cooperate with each other during the Targeted TI, RT test and Closure-phases. The TI provider and the RT provider need to get acquainted prior to the Launch meeting.

3.10 Risk management meeting [Meeting]

- **Responsible**: WT
- **Participants**: WT, TCT, (TI provider), (RT provider)
- **Preparation**:
    - TIBER-NO Risk Management Guidance
    - Risk Management Documentation, responsible: WT
        - Deadline: One week prior to the Risk management meeting
- **Meeting outcome**:
    - Walk-through of the Risk Management Documentation

The Risk management meeting should involve all the relevant stakeholders, including the TCT and the WT and optionally the TI and RT providers. In case of logistical restraints, remote participation can be arranged, but physical representation is preferred.

The final Risk Management Documentation should be made available to the TCT one week prior to the Risk management meeting. At the meeting, the WT lead presents the risk management controls, processes and procedures implemented by the WT to mitigate the inherent risk of a TIBER-NO test. The presentation should include the WT's agreements with the TI and RT providers regarding risk management This part could be presented by the TI provider and the RT provider, respectively.

The Risk management meeting will often be held in conjunction with the Scope meeting (*Scope meeting [Meeting]*).

3.11 Scope meeting [Meeting]

- **Responsible**: WT
- **Participants**: WT, TCT, TI provider, RT provider
- **Preparation**:
    - TIBER-EU Scope Specification, responsible: WT
        - Deadline: One week prior to the Scope meeting
- **Meeting outcome**:
    - Agree on the Scope Specification

The Scope meeting should involve all the relevant stakeholders, including the TCT, the WT, the TI provider, and the RT provider. In case of logistical restraints, remote participation can be arranged, but physical representation is strongly encouraged.

For the test to be successful, the TI provider and the RT provider need to understand the business of the entity. To enable this, the TI provider and RT provider are present at the Scope meeting.

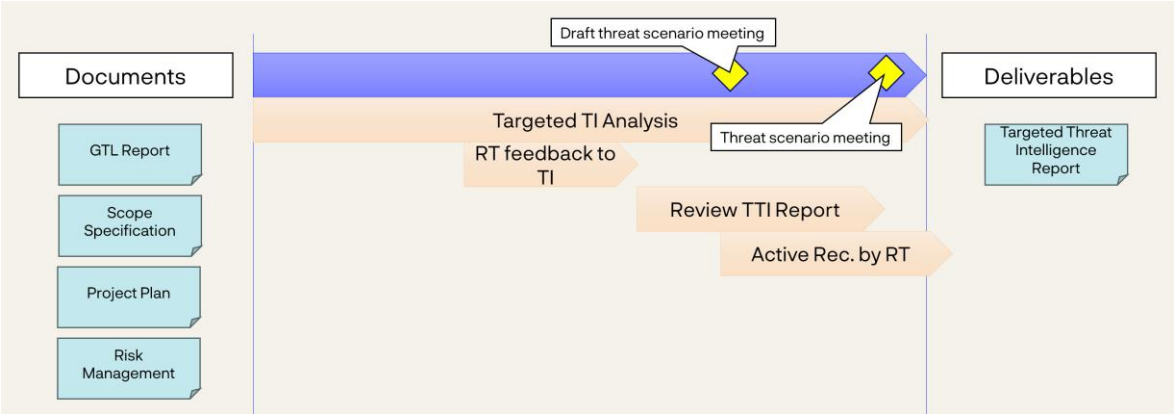
The final Scope Specification should be agreed-upon by the TCT during the Scope meeting. At the meeting, the WT lead presents the final scope and the methodology for selecting the critical functions, critical systems, processes and flags.

Following the Scope meeting, the agreed Scope Specification shall be approved and attested to by the entity's board.

The Scope meeting will often be held in conjunction with the Risk management meeting (*Risk management meeting [Meeting]*).

4 Targeted TI phase

The Targeted TI phase is the passive reconnaissance stage of the TIBER-NO test. To ensure actionable and relevant intelligence, the TI provider works closely with the RT provider. The main deliverable is the TIBER-NO Targeted TI Report on the entity, setting out threat scenarios for the test and useful information on the entity.



4.1 Targeted TI Analysis [Activity]

- **Responsible**: TI provider
- **Deliverable**:
  - Targeted TI Report
- **Documents**:
  - TIBER-EU Guidance for Target Threat Intelligence Report
  - Scope Specification
  - TIBER-NO Generic Threat Landscape Report

During the targeted threat intelligence process, the TI provider collects, analyses, and disseminates critical function-focused intelligence relating to two key areas of interest:

- Target intelligence - information on potential attack surfaces across the entity

- Threat intelligence - information on relevant threat actors and probable threat scenarios.

The targeted threat intelligence phase is strictly passive, and no active reconnaissance should be undertaken by the TI provider. Port scanning, phone calls, sending emails and linking on social media are all considered active reconnaissance. Activities like Google and dark web searches as well as browsing the entity's web pages are considered passive reconnaissance.

To identify targets (item 1 above), the TI provider should carry out a broad exercise of the kind typically undertaken by threat actors as they prepare for their attack from outside the network. The objective is to form a detailed preliminary picture of the entity and its weak points from the attacker's perspective, including weak points stemming from the use of third-party service providers (such as network, IT processing, software providers).

The output of the target identification is a description, on a critical function-focused, system-by-system basis, of the attack surfaces of roles, processes and technologies for the entity and its digital footprint. This includes information intentionally published by the entity and internal information that has been unintentionally leaked.

If the targeted intelligence points to threats or vulnerabilities that need immediate action and follow-up, this should be addressed according to the entity's process for risk management and not by the TIBER-NO test process.

Regarding threats (item 2 above), the TI provider should use the TIBER-NO Generic Threat Landscape Report as the basis for identification of relevant threat actors. With this starting point, the TI provider collects, analyses, and disseminates intelligence about relevant threat actors and probable threat scenarios. The objective is to present a credible picture of the cyber threat landscape, based on evidence-backed threat intelligence specifically tailored to the entity's business environment, including third-party service providers critical to the operation of the functions in scope.

The output from the threat identification is a summary of the key threats and detailed profiles of the most relevant threat actors.

Equipped with the output from target identification and threat identification, the TI provider is typically expected to produce three intelligence-led threat scenarios.

The threat scenarios are written from an attacker's point of view and emulate the attacker's capabilities. This means a detailed description of the emulated threat actor's preferred tactics, techniques and procedures, using the MITRE ATT&CK framework. To avoid the threat scenarios from being too much backward-looking, the TI provider should enhance each threat scenario with forward-looking plausible TTPs emulating what relevant attackers might be capable of in the foreseeable future. However, there should be a clear distinction between the evidence-based backward-looking scenarios vs. the hypothetical forward-looking TTPs in the described threat scenarios.

The result from the targeted threat intelligence process is a Targeted TI Report that should at least include the following three outputs:

- Tailored threat scenarios which will support the formulation of a realistic and effective Red Team Test Plan.
- Threat actor goals and motivations to help steer the RT provider in their attempt to capture the flags agreed upon in the Scoping activity.
- Validated evidence to underpin the business case for post-test remediation and improvement.

During the Targeted TI phase, based on draft threat scenarios, the RT provider might request the TI provider to obtain scenario-specific intelligence relevant for the attack. An example is information to be used directly for a spear phishing campaign.

The WT and the TI provider should schedule regular status meetings to ensure progress and alignment on the threat scenarios. The TCT will attend discussions on alignment of threat scenarios.

Once the TI provider has completed the Targeted TI Report, it should be shared with the WT, the TCT and the RT provider in a draft version at least one week before the Threat scenario meeting [Meeting]. The TCT will formally approve the Targeted TI Report, including threat scenarios.

4.2 RT Feedback to TI [Activity]

- **Responsible**: WT
- **Documents**:
    - Draft Targeted TI Report

The RT provider should be kept informed during the Targeted TI Analysis and provide feedback for the actionable intelligence and threat scenarios. In this context, the RT provider can request the TI provider to search for specific information that would help the RT provider operationalise and execute each threat scenario.

As the TI provider is limited to performing passive reconnaissance, the RT provider engages with the TI provider to manage expectations to the information held in the Targeted TI Report.

4.3 Review Targeted TI Report [Activity]

- **Responsible**: WT
- **Deliverable**:
    - Draft Targeted TI Report
- **Documents**:
    - TIBER-EU Guidance for Target Threat Intelligence Report
    - Scope Specification
    - TIBER-NO Generic Threat Landscape Report

The WT and TCT review the Targeted TI Report to verify whether the report lives up to the expectations outlined in the TIBER-EU Guidance for Target Threat Intelligence Report and the formal requirements from the TIBER-EU Framework document.

The actionable data to be used by the RT provider, e.g., the digital footprint of the entity, should be verified by the WT in order to not pursue non-existent possibilities in the RT Test phase.

4.4 Active reconnaissance by the RT [Activity]

- **Responsible**: RT

If deemed necessary by the WT, and with explicit consent from the TCT, the RT may commence non-intrusive active reconnaissance at a suitable point in time during the TI phase.

This potential head start of active testing activities has the purpose of accommodating stealthy reconnaissance without prolonging the test. The activity should be used to validate the passively collected intelligence, and the reconnaissance should directly support the RT's preparation of attack scenarios.

If active reconnaissance is performed during the Targeted TI phase, the RT is expected to share their findings with the TI provider to enable the information to be reflected in a separate section of the Targeted TI report.

During the active reconnaissance, it is imperative the RT takes the same precautions to remain undetected as they would take during the RT Test phase.

4.5 Draft threat scenario meeting [Meeting]

- **Responsible**: WT
- **Participants**: WT, TCT, TI provider, (RT provider)
- **Preparation**:
    - Draft Targeted TI Report, responsible: TI provider
        - Deadline: At the latest two days before the meeting
- **Meeting outcome**:
    - Agreement among all stakeholders on the draft threat scenarios

A Draft threat scenario meeting is held when a gross list of draft threat scenarios is ready. Attendees at the meeting are the WT, the TCT, the TI provider and (optionally) the RT provider. The TI provider explains the background for each threat scenario in draft, and together the participants evaluate the gross list and narrow it down to the two most relevant threat scenarios.

4.6 Threat scenario meeting [Meeting]

- **Responsible**: WT
- **Participants**: WT, TCT, TI provider, RT provider
- **Preparation**:
    - Draft Targeted TI Report, responsible: TI provider
        - Deadline: At the latest one week before the meeting
- **Meeting outcome**:

- Agreement among all stakeholders on the final threat scenarios

When threat scenarios are ready, a Threat scenario meeting is held, involving the WT, the TCT, the TI provider and the RT provider, during which the TI provider goes through the threat scenarios. At this point, only minor adjustments to the scenarios are expected, and the TCT will approve the Targeted TI Report, including the scenarios. After this meeting, the threat scenarios are delivered in a final version to be ready for the handover to the RT provider. The Targeted TI Report can be updated on an ongoing basis during the RT Test phase, if needed.

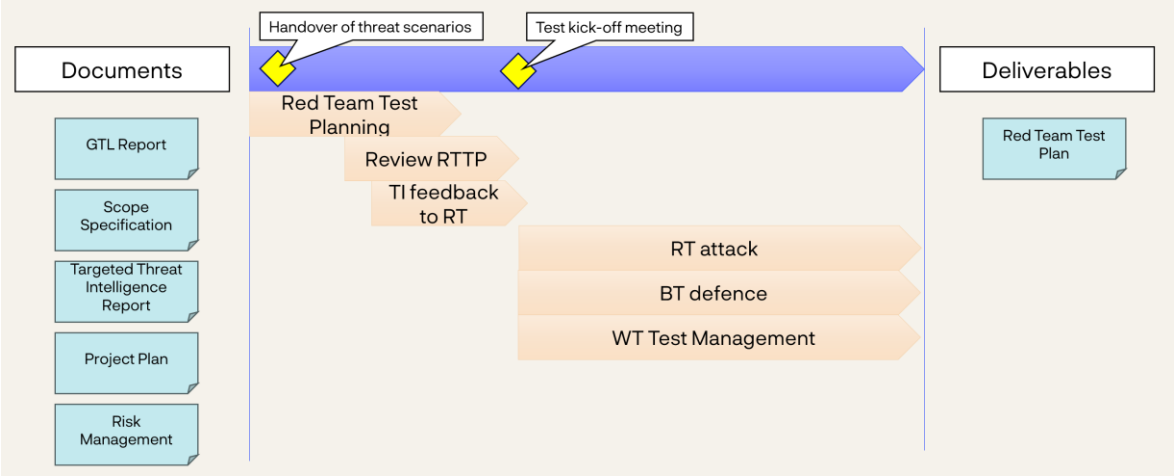
When the final threat scenarios are in place, the WT should revisit the WT composition to see whether this is sufficient given the critical functions/roles/processes/technologies included in the threat scenarios.

5 Red Team testing phase

Following the completion of the Targeted TI phase, the RT provider takes the lead. During the RT test phase, the RT provider plans and executes a TIBER-NO intelligence-led red team test of the target systems and services that underpin each critical function in scope.

Sufficient time should be allocated to the RT test phase to allow the RT provider to conduct a realistic and comprehensive test in which all attack phases are executed, and all test objectives are achieved. The test objectives agreed during the Preparation phase (and possibly updated during the Targeted TI phase) are the flags the RT provider must attempt to capture during the red team test as it progresses through the scenarios.

The time allocated for testing should be proportionate to the scope. Based on experience it is envisaged a total of 16 weeks (four weeks of preparation and 12 weeks of active testing) is a reasonable amount of time for the Red Team testing phase.



5.1 RT Test Planning [Activity]

- **Responsible**: RT provider
- **Deliverable**:
  - Red Team Test Plan
    - Deadline: Two days before the Test kick-off meeting
- **Documents**:
  - Scope Specification
  - TIBER-NO Generic Threat Landscape Report
  - Targeted TI Report
  - TIBER-EU Guidance for the Red Team Test Plan
  - TIBER-NO Red Team Test Plan Guidance

The intelligence-led attack scenarios are written from the attacker's point of view and should define specific targets to be reached, i.e., the flags to be captured, as defined in the Scope Specification. The RT provider should consider the TIBER-EU Guidance for the Red Team Test Plan and TIBER-NO Red Team Test Plan Guidance as well as the

Targeted TI Report, the TIBER-NO Generic Threat Landscape Report and the Scope Specification. This information and documentation provide the evidential basis for designing and justifying the proposed Red Team Test Plan and attack scenarios.

The RT provider should indicate various creative options in each of the attack phases based on various TTPs used by the 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 simply mimic scenarios seen in the past but combine the techniques of the various relevant threat actors.

Red Team testing should ideally for each scenario cover the phases initial access (IN), further intrusion into the organisation (THROUGH) and performing activities to support the goals of the threat actor (OUT). Testing can make use of leg-ups to progress scenarios ensuring each phase is tested to some extent.

The RT provider should align its test objectives with the goals of each of the threat actors, map these to the critical function-supporting systems, -roles and -processes, and produce credible real-life attack scenarios for the test. The attack scenarios are designed to provide background to the tradecraft employed by each threat actor to conduct a successful attack. The RT provider should adapt their attack methodology to replicate the real-life attack scenarios and apply this when designing and justifying the proposed RT Test Plan.

RT providers are constrained by available time and resources as well as moral, ethical and legal boundaries. It is hence possible the RT provider may require leg-ups from the WT to ensure the necessary progress. The RT provider should describe potential leg-ups in the test plan. The leg-ups should be discussed in advance with the WT and the TCT for the WT to start preparations for these as early as possible.

It is advised the WT arrange status meetings with the RT provider, the TCT and optionally the TI provider during the RT Test Planning to ensure progress and alignment with the scope, the threat intelligence, and the overall expectations of the attack plan.

Regarding attack scenario execution, the Red Team should consider whether to run scenarios in parallel or sequentially. Both have pros and cons. Parallel execution alleviates waiting periods, for example waiting for a phishing victim to click, but can sometimes risk detection as attacks are performed on multiple fronts. IT also requires the Red Team to plan the IN phase of the tests to be sufficiently similar. Sequential execution alleviates some of this risk, but potentially pushes the test period several weeks if success is limited. Additionally, if a scenario has to be revealed and proceed as a Purple Team test, it can be difficult to keep the other two scenarios secret. These are all factors the Red Team must consider when designing attack scenarios in the test plan.

The output of this activity is the final Red Team Test Plan, including attack scenarios to be followed. The TCT will formally approve the Red Team Test Plan (*Test kick-off meeting [Meeting]*).

5.2 Review RT Test Plan [Activity]

- **Responsible**: WT
- **Deliverable**:
  - Updates to Red Team Test Plan
- **Documents**:
  - TIBER-EU Guidance for the Red Team Test Plan
  - TIBER-NO Red Team Test Plan Guidance
  - Draft Red Team Test Plan
  - Targeted TI Report
  - Scope Specification
  - Risk Management Documentation

The WT and TCT review the Red Team Test Plan to make sure the plan meets the requirements in the TIBER-EU Guidance for the Red Team Test Plan and ensure the proposed actions are in accordance with the entity's risk appetite and the agreed-upon test scope.

5.3 TI Feedback to RT [Activity]

- **Responsible**: TI provider

The TI provider can be engaged during the red team attack. In real life, the attacker can leverage threat intelligence while attempting to compromise an entity. Allowing a fluid relationship between the TI provider and the RT provider during the red-team test may add value to the entity.

The TI provider can provide ongoing threat intelligence to the RT provider during the test, which may provide more useful reconnaissance and more insights in how to achieve the targets. Additionally, the TI provider may be consulted by the RT provider to assess whether a specific creative approach is in line with the simulated attacker's expected behaviour.

Additionally, the TI provider can give feedback to the Red Team Test Plan.

5.4 RT Attack [Activity]

- **Responsible**: RT provider
- **Input documents**:
  - Red Team Test Plan
  - TIBER-EU Purple Teaming Best PracticesTIBER-NO Red Team Status Reporting (PowerPoint)

The RT provider should deploy a range of TTPs during the test and follow a rigorous and ethical red team testing methodology. Irrespective of the methodology used by the RT provider, the test should be conducted in a controlled manner, taking a stage-by-stage approach in a way which does not bring unacceptable risks to the entity and its critical

functions. Risks to the entity, such as degradation of services, need to be kept to an absolute minimum and in accordance with the risk appetite.

During the execution of the test, the RT provider should perform a stealthy intelligence-led red team test of the target systems and services. The attack scenarios are not a prescriptive playbook to be followed precisely during the test. If obstacles or opportunities occur, the RT provider should show their creativity (as advanced attackers would) to develop alternative ways to reach the flag.

It is possible the RT provider may require occasional leg-ups from the WT to help them progress. Should this happen, the leg-up should be duly logged. The use of leg-ups ensures maximum benefit for all stakeholders.

The TCT should be updated at least once a week by the RT provider in status meetings, where the WT and preferably the TI provider participate. The WT and TCT should be kept updated of progress on an ongoing basis by the RT provider to be able guide the RT provider regarding which actions can and cannot be taken next, such as using the TIBER-NO Red Team Status Reporting (PowerPoint). If more frequent status meetings are held, for instance during the more critical phases of the attack, the TCT should be invited and participate when possible.

At critical points during the test (including leg-ups), the WT should be consulted by the RT provider before continuing the test, and the TCT should be informed immediately. Critical decisions (such as granting a leg-up) should be approved by non-objection by the TCT.

All the actions of the Red Team should be logged for the BT/RT replay workshop [Meeting] and as evidence for the Red Team Test Report.

Though the TIBER methodology ensures thorough planning, unexpected circumstances may arise during a live test forcing the stakeholders to act pragmatically to balance the objective of maximising the learning outcome against a strict interpretation of the framework.

A considerable amount of time and effort goes into the planning and execution of a TIBER test. An invalidation of the test for TIBER-NO recognition is not desirable, especially at the later stages of a test, unless violations of the framework have occurred. Therefore, in case exceptional and unexpected circumstances occur, there is a possibility for a purple teaming activity in the testing phase for the TIBER test to continue testing and maximise the entity’s return on investment.

The exceptional circumstances alluded to may vary on a case-by-case basis. The decision by the WT to include a purple teaming activity, upon non-objection by the TCT, is preceded by a thorough consideration of several alternative ways forward. For example, one should duly estimate if postponing the remainder of the test would maximise the lessons learnt. It is up to the TCT to evaluate each case individually in close dialogue with the entity, RT- and TI Provider and assess whether purple teaming activity is an option.

Purple teaming should not be considered a relaxation of the TIBER-NO requirements, but rather as a last resort option to ensure the highest possible learning outcome for the entity.

5.5 BT Defence [Activity]

- **Responsible**: BT (not informed about the test)

Not knowing that a test is being performed, the BT acts as usual and defends the entity to the best of their capability.

The test will likely require time and resources from the BT, i.e., BT response and escalation procedures as a reaction to RT activities. Therefore, in case a real cyber incident occurs during the test, the WT should assess if testing activities should be put on hold to avoid distracting the BT.

5.6 WT Test Management [Activity]

- **Responsible**: WT

During the RT attack, the workload on the WT can be intensive. The WT is expected to keep close communication with both the RT provider and the TCT to ensure the TIBER-NO test is conducted in a safe and controlled manner. As input to the activities in the Closure phase, it would be beneficial for the WT to keep a log of the attack seen from their point of view and a log of their own actions.

The WT must manage all possible escalations arising because of the test, for example if an event arises as part of the actions of the RT provider. For this, the WT should ensure sufficient arrangements are in place for the WT to be informed of actions taken by the BT, by the entity's security staff or by an external response capability.

5.7 Handover of threat scenarios [Mandatory meeting]

- **Responsible**: WT
- **Participants**: WT, TI provider, RT provider, (TCT)
- **Preparation**:
    - Targeted TI Report, responsible: TI provider
- **Meeting outcome**:
    - Formal handover of the final threat scenarios from the TI provider to the RT provider

Prior to the commencement of the test, the WT shall arrange a handover meeting, where the TI provider explains the Targeted TI Report and the threat scenarios in detail to the RT provider. The meeting may be skipped as it might not be needed if the RT provider has been closely involved in the Targeted TI phase. The TCT's participation in this meeting is optional.

5.8 Test kick-off meeting [Meeting]

- **Responsible**: WT
- **Participants**: WT, RT provider, TCT, TI provider
- **Preparation**:
    - Red Team Test Plan, responsible: RT provider
        - Deadline: Two days before the Test kick-off meeting [Meeting]
- **Meeting outcome**:
    - Formal launch of the RT attack and agreement on the Red Team Test Plan
    - Final alignment of rules of engagement and risk management

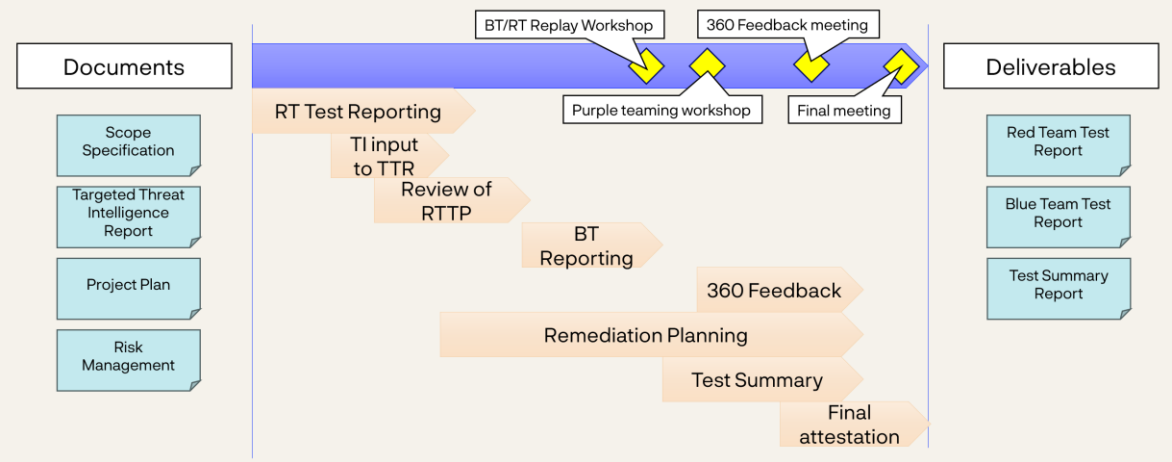
At this meeting, the RT provider presents the final Red Team Test Plan, including the attack scenarios to be carried out during the RT test. At this point, all stakeholders should be aligned, so only minor changes to the Red Team Test Plan should be needed, but the meeting can be used to clarify any remaining uncertainties regarding the test. Physical presence is encouraged. Risk management is revisited to make sure WT and RT provider expectations are aligned in this regard before the launch of the test. Any outstanding risk mitigation activities need to be addressed.

At the end of the meeting, the TCT formally approves the Red Team Test Plan and the commencement of the RT attack.

6 Closure phase

The Closure phase, including remediation planning and result sharing, allows all relevant stakeholders to reflect on the outcome of the test and make improvements to further enhance the cyber resilience of the entity.

Even though the test activities are concluded, this phase is relatively resource intensive on the part of the WT, as the WT is responsible for the production of a remediation plan and a test summary report as well as arranging the replay workshop and generally communicating and anchoring the results and learning points in their organisation.



6.1 RT Test Reporting [Activity]

- **Responsible**: RT provider
- **Deliverable**:
  - Red Team Test Report
    - Deadline: Two weeks after the conclusion of the RT Test phase
- **Documents**:
  - TIBER-EU Guidance for the Red Team Test Report

After the conclusion of the RT Test phase, the RT provider will draft a Red Team Test Report with details of the approach for to the testing as well as findings and observations from the test. The report is due two weeks after the conclusion of the RT Test phase, and the expected content of the report is described in detail in the TIBER-EU Guidance for the Red Team Test Report.

To verify the test has been conducted in line with the TIBER framework, the TCT will review the final Red Team Test Report on the entity's premises. The TCT does not store the report nor does the TCT share it or its content with anyone outside of the TCT. The review by the TCT is foreseen to take up to one full day.

6.2 TI Input to RT Test Report [Activity]

- **Responsible**: TI provider

- **Documents**:
    - Draft Red Team Test Report
    - Targeted TI Report

On request by the WT or RT provider, the Red Team Test Report may be enhanced with observations made by the TI provider. This may include, but is not limited to, justification of the chosen attack path from the TI provider's point of view.

6.3 Review of RT Test Report [Activity]

- **Responsible**: WT
- **Documents**:
    - Draft Red Team Test Report
    - TIBER-EU Guidance for the Red Team Test Report

The WT reviews the Red Team Test Report for the report to cover the requirements in the TIBER-EU Guidance for the Red Team Test Report and for the report to document the red team test and the results sufficiently. The WT should not alter the conclusions if the WT does not agree with these, since the WT can comment on such issues in the Test Summary Report.

6.4 Blue Team Reporting [Activity]

- **Responsible**: BT
- **Deliverable**:
    - Blue Team Test Report
        - Deadline: Before the *BT/RT replay workshop [Meeting]*
- **Documents**:
    - Red Team Test Report
    - TIBER-NO Blue Team Test Report Guidance

The key members of the entity's BT are informed of the test and will use the RT Test Report to deliver their own Blue Team Test Report. In the Blue Team Test Report, the BT maps its actions alongside the RT provider's actions. The BT can be informed and start writing the Blue Team Test Report as soon as the RT test execution is finalised. The Blue Team Test Report should be completed ahead of the *BT/RT replay workshop [Meeting]* to maximise the learnings from the replay.

6.5 360˚ Feedback [Activity]

- **Responsible**: TCT, WT, TI provider, RT provider, (BT)
- **Deliverable**:
    - Final TIBER-NO 360º Feedback Report
        - Deadline: One week after the 360˚ feedback meeting
- **Documents**:
    - TIBER-NO 360º Feedback Report

The goal is to further facilitate the learning experience of all those involved in the process for future exercises. All parties should deliver feedback on each other and on the overall process. For this purpose, the TIBER-NO 360º Feedback Report is used to collect feedback. The feedback from the WT, the TI provider, the RT provider and optionally the BT should be forwarded to the TCT at the latest two weeks before the 360˚ feedback meeting, and the TCT will send out an aggregated version to the participants one week in advance of the *360˚ feedback meeting [Meeting]*.

If deemed relevant by the WT, the BT can participate in the *360˚ feedback meeting [Meeting]*.

6.6 Remediation Planning [Activity]

- **Responsible**: WT/Entity
- **Deliverable**:
    - Remediation Plan
        - Deadline: Before the final Test Summary Report
- **Documents**:
    - Test Summary Report
    - TIBER-EU Guidance for the Test Summary Report
    - Targeted TI Report
    - Red Team Test Report
    - Blue Team Test Report

The entity drafts a Remediation Plan based on the test results, which should be used to support the business case for implementing improvements to mitigate the vulnerabilities identified during the TIBER-NO test. The plan may incorporate input and recommendations from the TI provider and the RT provider. The TCT will not review nor approve the Remediation Plan, but the remediation will be summarised in a section in the Test Summary Report.

6.7 Test Summary Reporting [Activity]

- **Responsible**: WT
- **Deliverable**:
    - Test Summary Report
        - Deadline: One week before the Final Attestation [Activity]
- **Documents**:
    - TIBER-EU Guidance for the Test Summary Report
    - Scope Specification
    - Targeted TI Report
    - Red Team Test Plan
    - Red Team Test Report
    - Blue Team Test Report
    - Remediation Plan

The Test Summary Report summarises the overall test process and results (including the Remediation Plan) and should draw on the above documents. The Test Summary Report should not contain detailed technical information and findings regarding weaknesses and vulnerabilities, as information at that level of detail is highly sensitive and for the entity only. The entity must share the Test Summary Report with the TCT for review and approval, including the final version.

The entity is encouraged to share effective remediation and best practices, for instance with the TIBER-NO community, since the main goal of TIBER is to enhance the cyber resilience of the Norwegian financial sector.

The TCT will not share any information or documentation from the test with any outside party. However, the TCT may use the anonymised results of the Test Summary Report to share general knowledge with the other entities in the TIBER-NO programme and to improve the TIBER-NO and TIBER-EU frameworks. This includes cooperation with the TIBER Knowledge Centre and with other national TCTs to identify common vulnerabilities across different TIBER-EU tests to help to form a picture of the resilience level of the European financial sector and bring about improvements, where feasible. Information will only be shared if/when a critical mass of anonymised findings/vulnerabilities is identified, such that the anonymity of the individual test can be maintained definitively.

6.8 Final Attestation [Activity]

- **Responsible**: WT, TCT, RT provider, TI provider
- **Deliverable**:
    - Signed TIBER-EU Attestation Template
        - Deadline: One week after the final Test Summary Report
- **Documents**:
    - TIBER-EU Attestation Template

At the end of the test, once the reports and the Remediation Plan have been agreed upon, the entity, the TI provider, the RT provider and the TCT should provide an attestation confirming the test was conducted in accordance with the core requirements of the TIBER framework. The attestation document will be reviewed at the status meetings as the test progresses to ensure no issues will arise in the final attestation process.

The TIBER-EU Attestation Template should be signed by the board/high-level executive management of the entity and at the TI provider and the RT provider to serve as a means of qualifying the test for mutual recognition among other relevant authorities.

6.9 BT/RT replay workshop [Meeting]

- **Responsible**: WT
- **Participants**: WT, RT provider, TCT, BT, (TI provider)
- **Preparation**:
    - Plan the content of the BT/RT replay workshop with the RT provider, responsible: WT

    - Prepare the BT/RT replay workshop, responsible: RT
- **Meeting outcomes**:
    - Overview of the test outcome (broad audience)
    - Step-by-step presentation of the test from an RT point of view (narrow audience)
    - RT recommendations for remediation

After the RT provider and the BT have delivered their reports, the WT must arrange a BT/RT replay workshop. The goal of this workshop is to learn from the testing experience in collaboration with the RT provider. During the workshop, a replay is organised in which the BT and the RT provider review the steps taken by both parties during the test. The BT/RT replay workshop is foreseen to stretch over approximately two days.

Prior to the BT/RT replay workshop, the BT and RT must agree on the timeline of events during the executed test. This is necessary to facilitate a meaningful replay and discussion about the actions taken by the BT and RT during the test.

When conducting the replay, the RT provider should state how the testing team managed to progress through the targeted attack life cycle stages of each scenario. The RT provider should 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 resource limitations of TIBER.

Furthermore, the WT should consider involving the TI provider in the replay/follow-up with focus on improving the intelligence capability of the entity, for instance by having a deep dive into the chosen threat actors at the BT/RT replay workshop.

6.10 Purple teaming workshop [Optional meeting]

- **Responsible**: WT
- **Participants**: RT provider, BT, (TI provider)
- **Preparation**:
    - Prepare purple teaming activities with the WT and the BT, responsible: RT provider.
- **Meeting outcome**:
    - Training of the BT capabilities and processes

A purple teaming element can be added to the Closure phase as an extension of the replay, in which the BT and the RT provider work closely together to see which other steps (in systems or processes) could have been taken by the RT provider, and how the BT could have responded to those steps.

Purple teaming can also cover table-top exercises based on the RT test outcome playing out 'what if' scenarios with relevant business experts and other members of the BT.

The purple teaming workshop is an opportunity to train the BT's protect, detect and response capability and to evaluate the existing processes and system monitoring tools.

6.11 360˚ feedback meeting [Meeting]

- **Responsible**: TCT
- **Participants**: WT, TI provider, RT provider
- **Preparation**:
    - Input to TIBER-NO 360º Feedback Report, responsible: WT, TI provider, RT provider
        - Deadline: At the latest two weeks before the 360˚ feedback meeting
    - Input to and draft 360˚ Feedback Report, responsible: TCT
        - Deadline: One week in advance of the 360˚ feedback meeting
- **Meeting outcomes**:
    - Input to final TIBER-NO 360º Feedback Report

A 360˚ feedback meeting is held between the WT, the TCT, the TI provider and the RT provider to review the TIBER-NO test. The TCT should arrange and facilitate the meeting. Physical representation is strongly encouraged; however, in case of logistical restraints, remote participation can be arranged. At the 360˚ feedback meeting, all parties should deliver feedback on each other and on the overall process on the basis of the TIBER-NO 360º Feedback Report.

The TCT may share the output from the TIBER-NO 360º Feedback Report on an anonymous basis with the TIBER Knowledge Centre, so all lessons learnt can be reflected on and improvements can be made to the TIBER-EU framework. This is a key part of the 'learning and evolving' principle that underlies the TIBER frameworks.

6.12 Final meeting [Meeting]

- **Responsible**: TCT
- **Participants**: WT
- **Meeting outcomes**:
    - Closure of the TIBER-NO test process for the Entity

At the end of the test process, a final meeting between the TCT and the WT is held to formally close the test process and to discuss the timing of the entity's next TIBER-NO test. For instance, any outstanding points in the action log will be closed and an agreement on when to close down the common document folders will be made. Also, how to share the learnings, which can be used by other organisations to enhance cyber resilience, may be discussed.

Appendix A: RACI-matrix of deliverables and meetings

This matrix references Table 5 from the TIBER-EU Framework "1.2 Responsibility Assignment Matrix for a TIBER-EU test" and has been adapted to fit the TIBER-NO implementation. The S for Support has been omitted to decrease complexity and because the supportive work is largely performed as consulting (C) by the TCT.

R – responsible, A – accountable, C – consulted, I – informed. (* means optional)

SP is for Service Provider (critical supplier for the entity, not to be confused with TI/RT-providers), part of the WT but nonetheless included as its own role for the purpose of clarifying their involvement.

Name	Phase	TCT	WT	SP	TI	RT	BT
Error! Reference source not found.	Initiation	C	R, A	C			-
Project Planning [Activity]	Initiation	C	R, A	C			-
Initiation meeting [Meeting]	Initiation	R, A	C	C			-
Scoping [Activity]	Preparation	C	R	C			-
Procurement [Activity]	Preparation	C	R	C			-
Risk Management [Activity]	Preparation	C	R	C			-
Input to Targeted TI [Activity]	Preparation		R	I	C		-
TI Preparation [Activity]	Preparation		C		R		-
RT Preparation [Activity]	Preparation		C		I	R	-
Pre-launch meeting [Meeting]	Preparation	R	C	C			-
Scoping workshop [Meeting]	Preparation	R	C	C			-
Launch meeting [Meeting]	Preparation	C	R	C	I	I	-
Scope meeting [Meeting]	Preparation	C	R	C	C	C	-
Risk management meeting [Meeting]	Preparation	C	R	C	C	C	-
Targeted TI Analysis [Activity]	Targeted TI	C	I		R	I	-
RT Feedback to TI [Activity]	Targeted TI		C	C	C	R	-
Review Targeted TI Report [Activity]	Targeted TI	C	R				-
Active reconnaissance by the RT [Activity]	Targeted TI	I	C			R	-
Draft threat scenario meeting [Meeting]	Targeted TI	C	R	I	C	I*	-
Threat scenario meeting [Meeting]	Targeted TI	C	R	I	C	I*	-
RT Test Planning [Activity]	RT Test	C	C	C	C	R	-

Name	Phase	TCT	WT	SP	TI	RT	BT
Review RT Test Plan [Activity]	RT Test	C	R	C	C		-
TI Feedback to RT [Activity]	RT Test	C	C		R	I	-
RT Attack [Activity]	RT Test	C	C	C	C	R	
BT Defence [Activity]	RT Test	I	I				R
WT Test Management [Activity]	RT Test	C	R				
Handover of threat scenarios [Mandatory meeting]	RT Test	I*	R		C	I	
Test kick-off meeting [Meeting]	RT Test	C	R	I	I	C	
RT Test Reporting [Activity]	Closure	C	C		I	R	
TI Input to RT Test Report [Activity]	Closure	I	I		R	C	
Review of RT Test Report [Activity]	Closure	C	R		I	C	
Blue Team Reporting [Activity]	Closure	C	C			C	R
360˚ Feedback [Activity]	Closure	R	C	I*	C	C	C
Remediation Planning [Activity]	Closure	I	R	I*		C	C
Test Summary Reporting [Activity]	Closure	C	R			C	
Final Attestation [Activity]	Closure	R	C	C	C	C	
BT/RT replay workshop [Meeting]	Closure	C	R	C*	C*	C	C
Purple teaming workshop [Optional meeting]	Closure	C	R	I	I	C	C
360˚ feedback meeting [Meeting]	Closure	R	C	C	C	C	C
Final meeting [Meeting]	Closure	R	C	-	-	-	-

Appendix B: Change log

Version	Date	Change
1.3	11.06.2024	AH: Added and updated document references. Updated phase illustrations. Added generic agenda for status meetings in section 3.7 Pre-launch meeting. Added paragraph on scenario execution in section 5.1 RT Test Planning. Smaller editorial updates.
1.2.1	25.10.2023	AH: Added sentence on internal RT in section 3.2. Updated external document references.
1.2	05.10.2023	AH: Merged contents form “Test Process Overview” into chapter 1. Changed chapter numbering. Added section 1.5 Documents and updated document reference consistency throughout. Bookmarks and links added to documents and headings. Added contacting FSA in 3.3 Risk Management.

		Added IN-THROUGH-OUT in 5.1 RT Test Planning. Added this Change log as Appendix B. Numerous editorial updates.
1.1	21.03.203	AH: Language reverted back to English. Added RACI matrix as Appendix A. Minor editorial and formatting updates.
1.0	01.01.2023	AH: Initial version translated to Norwegian based on document from TCT-DK