TIBER-NO

Operational Guide

Version 2.3.1 – 26 October 2026



Contents

1 Introduction 3
1.1 Background 3
1.2 TIBER-NO test process overview 3

2 Preparation phase 5
2.1 Notification process 5
2.2 Initiation process 7
2.3 Scoping process 10
2.4 Procurement process 15
2.5 Approval process 19
2.6 Project management process 20

3 Testing phase: Threat intelligence 23
3.1 Threat intelligence collection process 23
3.2 Scenario creation process 25
3.3 TTI Report creation process 27
3.4 Approval process 29
3.5 Project management process 30

4 Testing phase: Red-Teaming 32
4.1 RT test plan creation process 32
4.2 Approval process 35
4.3 Active Testing process 36
4.4 Project management process 40

5 Closure phase 42
5.1 RT & BT reporting process 43
5.2 Replay process 45
5.3 Purple Teaming process 46
5.4 Approval process 48
5.5 360° Feedback process 49
5.6 Reporting process 51
5.7 Attestation process 54
5.8 Project management process 55

Appendix A: Abbreviations 57

Appendix B: Change log 58

1 Introduction

1.1 Background

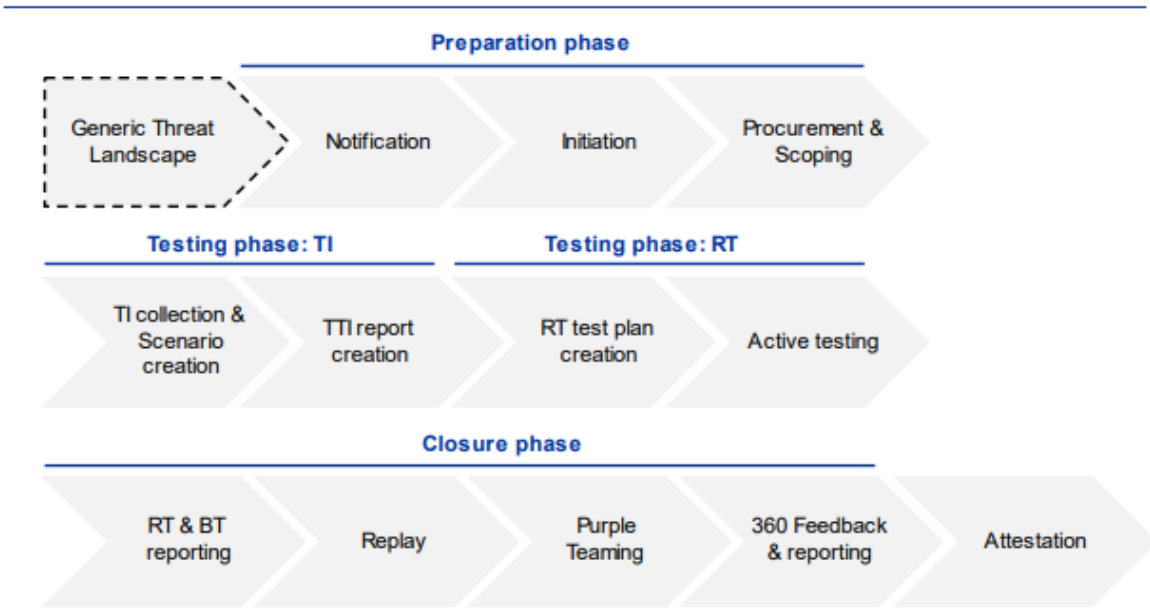
This guide, the TIBER-NO Operational Guide, provides a step-by-step description of each of the elements in the TIBER-NO test process. This Operational Guide refers to documents common to TIBER-EU and documents specific for TIBER-NO. The TIBER-NO Implementation Guide describes how the requirements in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

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

1.2 TIBER-NO test process overview

The TIBER-NO test processes follow the same processes as TIBER-EU.



The test is in TIBER-EU divided into 4 different phases: preparation phase, the testing phase: TI, the testing phase: RT and the closure phase.

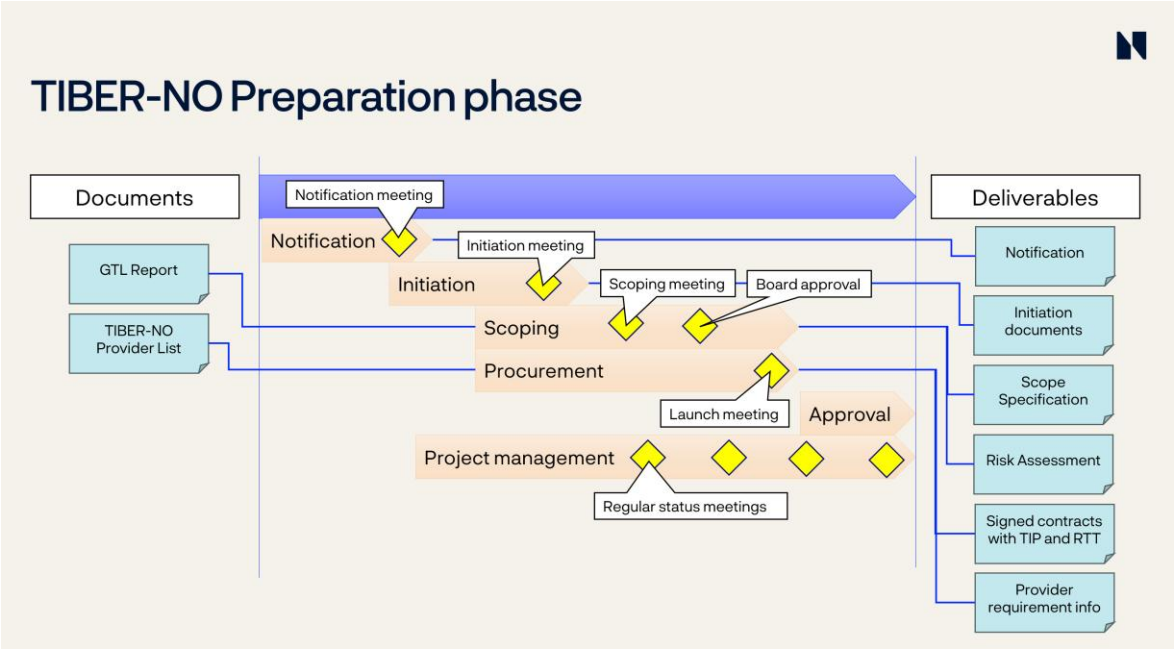
For each phase a set of processes are defined. In TIBER-NO, this is mainly based on the same processes as in TIBER-EU with the addition of “Project Management” for each phase. In addition, this operational guide details activities for each process. These activities include the elements from TIBER-EU, requirements form DORA and the DORA Regulatory Technical Standard for TLPT, and activities and guidance based on experiences from previous TIBER tests.

For further guidance of individual activities and deliverables, there are a set of TIBER-NO and TIBER-EU guidance documents and templates. For each activity described in this operational guide, there are references to the relevant sections of TIBER-EU, DORA and TIBER-NO guides and templates.

To clearly show important information in this guide, several boxes with different colours are included. The structure of the coloured boxes are as follows:

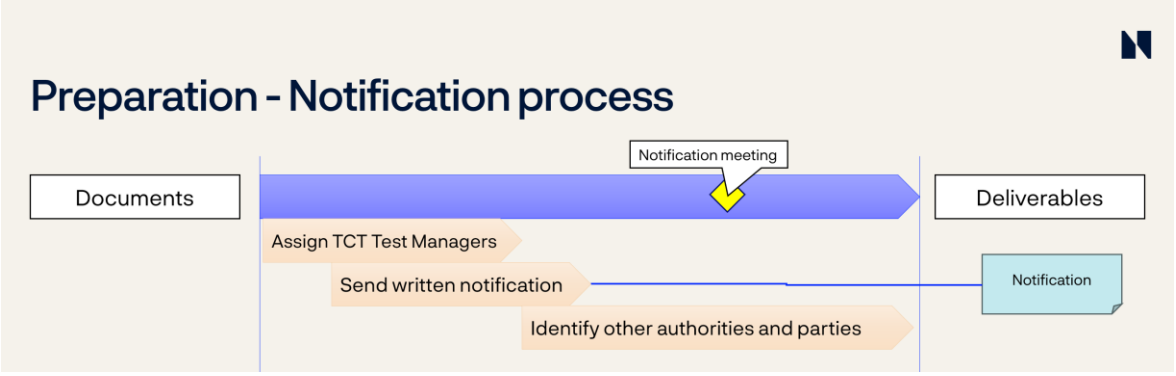
- Green: Recommended guides and deliverable documents.
- Blue: Meetings.
- Orange: Responsible stakeholder for activities, deadlines for specific activities, references to TIBER-EU, DORA and DORA RTS requirements for the specific activities.

2 Preparation phase



The preparation phase is key to a successful TIBER-NO test and typically is the longest of all phases. Thorough preparations before the actual test ensures a smooth and controlled test giving maximum amount of learning and value from the test. The preparation phase is scheduled for maximum 6 months from the starting date stated in the notification from the TIBER authority to the entity. The approval process comes in addition and may not be included in those six months.

2.1 Notification process



The notification process initiates the TIBER and sets up the basis for the test. The written notification from the TCT marks the formal start of the TIBER test and deadlines for completing other processes relate to the start date set in the notification which is sent to the entity performing the TIBER test.

The TCT is strongly encouraged to contact the entity as early as possible, ideally well before the above-mentioned written notification. This is to discuss and coordinate when the test will start, also keeping in mind a lengthy procurement and scoping process. Moreover, potential resource and budget constraints need to be anticipated by the entity.

Relevant documents for this process

- TIBER-NO General Implementation Guide
- TIBER-NO Operational Guide
- TIBER-NO Test Overview (Excel)
- TIBER-NO Notification Letter
- TIBER-EU Control Team Guidance
- TIBER-EU Guidance for Server Provider Procurement
- TIBER-EU Scope Specification Document Guidance

Deliverables

- Notification Letter

2.1.1 Assign TCT Test Managers

The TCT shall plan and assign Test Managers to follow the rest. Typically, one TM will be assigned as the responsible TM and will function as the primary point of contact towards the entity. In addition, one or two additional TMs shall be assigned to ensure stability and continuity of the test from the TCT.

Responsible: TCT
References:
- TIBER-EU 6.1
- RTS Art. 3(2)

2.1.2 Send written notification

The TCT sends a written notification to the entity to be tested, marking the start of the test and indicating the requirements to be followed during testing. The contact details of the TCT should also be communicated in this notification.

Responsible: TCT
References:
- TIBER-EU 6.2
- RTS Art. 3(4), 8(1) and 9(1)

The tasks of the entity in the preparation phase should be finished within a maximum of six months after the start date stated in the written notification.

2.1.3 Notification meeting

Each TIBER engagement starts with a notification meeting for which the TCT is responsible. The main outcome of the meeting is to understand the TIBER framework and give a basis for the planning of the test. There should be sufficient time for allocation of resources for the test, both for the entity and the TCT. The TCT can provide suggestions for dates of the different parts of the test in the TIBER-NO Test Overview (Excel).

Responsible: TCT
Participants: Entity
Type: Physical
Typical duration: 2 hours
References: TIBER-EU 6.2

The notification meeting takes place with, or shortly after the written notification.

During the meeting, the Test Manager will brief the entity on:

- Its designation to carry out a mandatory or voluntary test
- Stakeholder roles and responsibilities
- Testing process, its elements and deliverables
- TCT and CT composition.

Preparation

- Be familiar with TIBER-EU, TIBER-NO and, if applicable DORA TLPT and DORA RTS for TLPT.

Agenda

- Notification, Implementation Guide, Operational Guide and Test Process Overview
- Introduction to Initiation Documents
- Identify possible entities or legal parties involved in the test
- Introduction to Procurement, Scope and Risk Management

Outcomes

- Formal notification to conduct a TIBER-NO test
- Alignment on TIBER-NO Test Process Overview
- Familiarisation with the TIBER-NO test process
- Preparation for producing the Initiation Documents
- Early start of procurement
- Initiation meeting planned

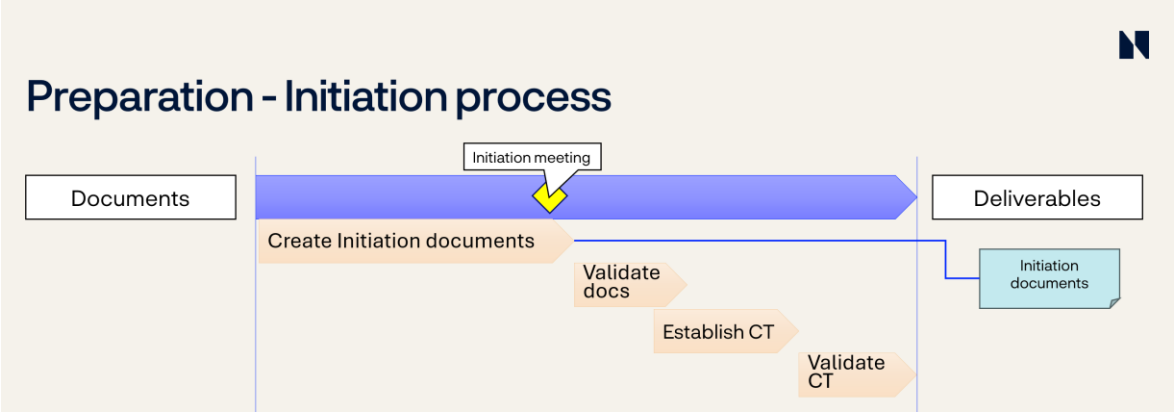
2.1.4 Identify other authorities and parties

Responsible: TCT
References: TIBER-EU 6.2

As early as possible but no later than the validation of the initiation documents by the Test Manager, other authorities or legal parties which might be included in the test should be identified. The TCT responsible for leading the test should inform other possible relevant authorities about the test.

The tested entity should confidentially inform all the other relevant legal parties to be included in the test, such as subsidiaries, Critical Service Providers, etc. The TM briefs all parties involved on the steps in the TIBER-EU process, documentation, stakeholder roles and responsibilities.

2.2 Initiation process



The initiation process is the start of the active planning process of the TIBER test.

During the initiation process, the entity first identifies a responsible Control Team Lead. The CTL prepares the initiation documents, which include a project charter, comprising a high-level project plan and communication details and channels to be established. The code name for the TIBER test is determined. The CTL then puts together the Control Team. The information regarding any planned or ongoing test is limited on a need-to-know basis, including the management body of the entity. However, the CT must ensure the management body of the entity is informed about the progress of the test and its associated risks.

Relevant documents for this process

- TIBER-NO General Implementation Guide
- TIBER-NO Operational Guide
- TIBER-EU Control Team Guidance
- TIBER-NO Test Overview CT (Excel)
- TIBER-EU Initiation Documents Guidance
- DORA – Regulation 2022/2554 on digital operational resilience for the financial sector
- DORA RTS for TLPT and DORA RTS for TLPT Annex
- TIBER-NO Approval Checklists
- TIBER-EU Guidance for Service Provider Procurement

Deliverables

- Initiation documents

The CTL shall send the initiation documents to the TM no later than 3 months after the written notification.

The initiation documents will be presented by the CTL in the initiation meeting and are subsequently assessed and validated by the TM.

2.2.1 Create initiation documents

The entity may use its own format for the initiation documents. The content of the plan can be based on the plan found in the TIBER-NO Test Overview (Excel) and the dates agreed upon with the TCT. The initiation documents must include a schedule of meetings to be held between the CT, TIP, RTT and the TCT to review deliverables.

The requirements for the minimum contents of the initiation documents are detailed in:

- TIBER-EU Initiation Documents Guidance
- DORA RTS for TLPT article 9(2) and Annex I

Responsible: CTL
Deadline: 3 months after written notification
References:
- TIBER-EU 6.3
- TIBER-EU Initiation Documents Guidance
- RTS Art. 9(2), 15(3) point (a) and Annex I

Once the initiation documents are completed, they should be presented at the initiation meeting and submitted to the TM for validation.

2.2.2 Initiation meeting

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

Responsible: CTL
Participants: TM
Type: Physical or online
Typical duration: 1 - 2 hours
Deadline: 3 months from written notification
References: TIBER-EU 6.3

During the initiation meeting, the CTL should brief the TM on:

- the content of the initiation documents
- the planned composition of the CT
- contractual considerations regarding procurement
- initial efforts undertaken to manage the risks of the test

Regular status meetings between the CT 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 CT. Status meetings shall be held approximately every fortnight in the preparation phase and may be supplemented with additional meetings as needed.

Preparation

- Entity prepares suggestion for code name for the test
- Initiation documents

Agenda

- CTL briefs TM on the initiation documents

Outcomes

- Plan for regular status meetings with CT and TCT
- Discuss Initiation Documents
- Agree on code name

2.2.3 Validate initiation documents

When the TM receives the initiation documents, they should be validated to ensure the documents are complete and all minimum requirements are met. This is to ensure the suitability and effective performance of the test. The TIBER-NO Approval Checklists for initiation documents should be used by the TM. After the initiation documents are successfully validated and complete, the TM shall notify the CTL of its validation.

Responsible: TM
References:

- TIBER-EU 6.3
- RTS Art. 9(3)

2.2.4 Establish Control Team

As part of the initiation process the entity must establish the CT, which is the management group for the TIBER-NO test. The entity must follow the TIBER-EU Control Team Guidance to establish a CT.

Responsible: Entity
References:

- TIBER-EU 6.3
- RTS Art. 4(1), 9(4) and 9(5)

The CT should be kept to a minimum to make it easier to maintain the secrecy of the test and make the project planning easier.

This team comprises a select number of individuals who have critical decision-making capacity, and/or are experts, e.g. cyber, operational and risk specialists, experts from the business areas supporting the Critical and Important Functions (CIFs), project management etc. Members of the CT are positioned in the entity such that they have access to the top of the security incident escalation chain. The composition of the CT can be flexible, depending on the specific structure and organisational set-up of the entity. The CTL makes sure the CT is aware of the TIBER test, the need for secrecy and the process the CT should go through in case the BT detects and escalates a TIBER-related incident.

Due to the sensitive nature of the preparation and execution of the TIBER-NO test, the entity can consider if CT members should sign a non-disclosure agreement to ensure internal and external confidentiality of the test.

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

2.2.5 Validate composition of Control Team

The TM validates the initial composition of the CT, based on evaluating if it is adequate for the performance of the tasks it is responsible for.

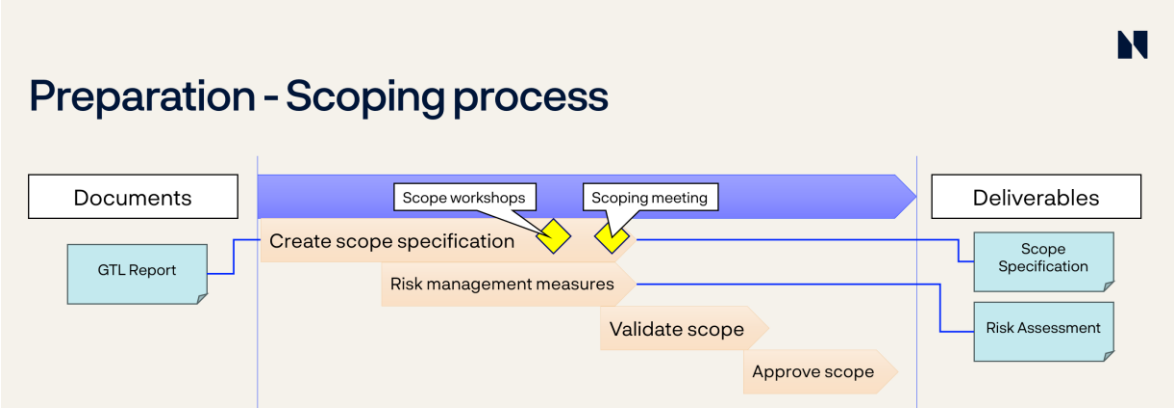
Responsible: TCT
References:

- TIBER-EU 6.3
- RTS Art. 9(5)

The TM shall inform the CTL of its validation.

Any subsequent changes to the CT shall be evaluated by the TM and the CTL informed.

2.3 Scoping process



During the scoping process step, the tested entity shall complete a TIBER-EU Scope Specification Document (SSD), describing Critical and Important Functions (CIFs), systems and services supporting each CIF, and possible flags to be captured.

The key objective of the scoping process is for the involved entities to select, and for the TM to validate, the CIFs to be included in the test.

The definition of a CIF in TIBER-EU is defined under DORA Article 3(22) as "*a function, the disruption of which would materially impair the financial performance of a financial entity, or the soundness or continuity of its services and activities, or the discontinued, defective or failed performance of that function would materially impair the continuing compliance of a financial entity with the conditions and obligations of its authorisation, or with its other obligations under applicable financial services law.*"

Flags are objectives to ensure the testing of critical and important functions gives the best possible learning and actively guides the test in the right direction in each phase. This can for example be *"obtaining sufficiently high user privileges to initiate transactions through the SWIFT system"*. Flags shall be updated throughout the test, becoming more detailed and specific as the test progresses.

In the Scope Specification Document, the CT documents for the first time the flags they consider relevant for the test. These flags are preliminary and serve as a starting point for the TIP and RTT. Flags shall be evaluated and updated by the CT throughout the whole testing process until active testing is completed. Capturing flags is not an indicator of a successful TIBER test. Setting flags is a challenging process, and sufficient effort must be invested in defining good flags that give the entity the learning and answers it is seeking.

Flags are further defined and adjusted in the Targeted Threat Intelligence Report (section 3.2 and 3.3) and the Red Team Test Plan (section 4.1).

Relevant documents for this process

- TIBER-EU Scope Specification Document Guidance
- TIBER-NO Risk Management Guidance
- TIBER-NO Generic Threat Landscape Report

Deliverables

- Scope Specification Document
- Risk Management Documentation

Throughout the entire TIBER test, having a consistent naming convention makes communication easier and reduces misunderstandings. We suggest using the following:

Component	Code	Example
Critical functions	CF-[number]	CF-01
Scenarios	SC-[letter]	SC-A
Flags	FL-[scenario-letter]-[number]	FL-A-01 (for scenario A)
Leg-ups	LU-[scenario-letter]-[number]	LU-A-01 (for scenario A)
Risks	RI-[number]	RI-01

2.3.1 Create scope specification

Responsible: CT
Deadline: 6 months after written notification
References:
- TIBER-EU 6.4
- DORA Art. 26(2) and 26(3)
- RTS Art. 9(6) to 9(9) and Annex II

Entities may conduct a business impact analysis defining the CIFs as part of their standard business continuity management or operational risk management practices, which may be used as input. This might typically have been performed already, such as for other areas of DORA. Even though CIFs are scoped within a test, this does not mean all these CIFs are actively targeted in the testing phase, as this is contingent on the threat intelligence and ultimately the attack scenarios and attack path of the RTT. The entity may also refer to the GTL Report for examples and to further contextualise its business and the threats it faces. In practice, this means the scope should be wide and cover all critical and important functions of the entity, while what will be tested will only be a subset of this scope.

For each CIF, the underlying systems and processes should be included in the Scope Specification Document as well. These should be clearly linked together.

For each CIF in scope, the CT should set at least one “flag” to be captured during the test. A flag is essentially the objective the RTT must strive to achieve during the test, e.g. compromising the confidentiality, integrity, or availability of the target system. 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. The flags set in this process is therefore just a starting point. It is recommended to have at least one flag per IN-THROUGH-OUT phase of each scenario, based on the Unified Kill Chain model.

Once contracted, the CT shall share the SSD with the TIP and RTT.

The SSD must be delivered by the entity to the TM within six months from the start date sat in the written notification and should be approved by the management body of the entity.

2.3.2 Scope workshops (optional meetings)

Responsible: CT
Participants: TCT
Type: Physical or online
Typical duration: 2 hours
References: TIBER-EU 6.4

To ensure a good start of the scoping activity, one or more scoping workshops may be arranged to discuss the scope of the test.

In preparation for the scoping workshops, the CTL should create a gross list of the entity's Critical and Important Functions (CIFs) and investigate how they depend on critical IT systems, roles and processes. For this purpose, for example high-level system architecture diagrams or similar should be acquired to provide an overview of the entity's critical systems supporting the CIFs.

At the scoping workshop, the CT presents the CIFs and explain the high-level system landscape of the entity to the TCT. It may be relevant to include subject matter experts with extensive insights into both the business and IT side of the entity.

The outcome of the scoping workshop is to identify the entity's CIFs, its supporting key systems, processes, and potential flags. This will then be the basis for the contents of the SSD and the scoping meeting.

Preparation:

- Gross list of CIFs
- High-level system architecture
- Critical business processes

Agenda:

- Discuss CIFs
- High-level system landscape
- Walkthrough of draft Scope Specification Document

Outcomes:

- Identification of the entity's CIFs, its supporting systems, processes and potential flags.

2.3.3 Risk management measures

Responsible: CT
References:

- TIBER-EU 4 and 6.4
- DORA Art. 26(5)
- RTS Art. 4(2), 5(1), 5(2) and 9(10)

Prior to the testing phase, the CT should consult the TM on the risk assessment and risk management measures. The CT shall review the risk assessment and risk management measures in case the TM assesses they do not adequately address the risk of the TIBER test. Moreover, the CTL should regularly assess the risks and the related mitigation measures throughout the test.

Ultimately, the entity is responsible for the red team test and the risks that stem from it. The CT should therefore remain in control of the testing process, as well as continuously manage the relevant risks in an effective manner.

The CT should conduct a risk assessment before and during the test. The risk assessment should be well documented, reviewed and updated when needed, such as when the attack scenarios have been developed. Before the testing phase commences, the CT should consult the TM on the risk assessment. Risks to be considered – among others – relate to:

- Procurement of providers
- Level of confidential data to which these providers gain access
- Crisis and incident escalation
- Interruption of critical activities and/or impact of provider activities on the entity and its third parties
- Incomplete restoration of systems affected by the test

See TIBER-NO Risk Management Guidance and TIBER-EU Framework chapter 4 for further details.

2.3.4 Scoping meeting

The CT shall organise a scoping meeting to discuss the scope of the test with the TM, as well as the TIP and RTT, if already procured. If applicable, feedback on the test scope might also be provided by other TIBER authorities and the entity's supervisors/overseers. As a minimum, the CT should discuss the flags with the TM, who must be involved throughout the scoping process.

Responsible: CT
Participants: TCT, (TIP, RTT)
Type: Physical is encouraged
Typical duration: 2 hours
References: TIBER-EU 6.4

In this meeting, risk management measures and documentation should also be presented by the CT.

Following the scoping meeting, the SSD shall be approved and attested to by the entity's board.

The scoping meeting takes place after the initiation meeting, but no later than six months after the written notification.

Agenda

- Discuss the scope of the test, including feedback by the TCT
- Walk-through of the risk management measures and documentation

Outcomes

- Feedback on Scope Specification Document

For the test to be successful, the TIP and the RTT need to understand the business of the entity. To enable this, the TIP and RTT should be present at the Scoping meeting. If the TIP or RTT are not yet procured, the CT shall update them on the scope at a later date.

2.3.5 Validate scope

When the TM receives the Scope Specification Document, it shall be checked towards the formal requirements. The TIBER-NO Approval Checklists for Scope should be used by the TM.

If the test is a TLPT, the TM shall discuss the CIFs in scope with Finanstilsynet before validation. Finanstilsynet shall be given the opportunity to comment.

Responsible: TCT
References:

- TIBER-EU 6.4
- RTS Art. 9(12)
- DORA forskriften §13

After the documents are successfully validated and complete, the TM should notify the CTL such as by filling out the completed checklist and informing the CTL of the validation.

2.3.6 Approve scope

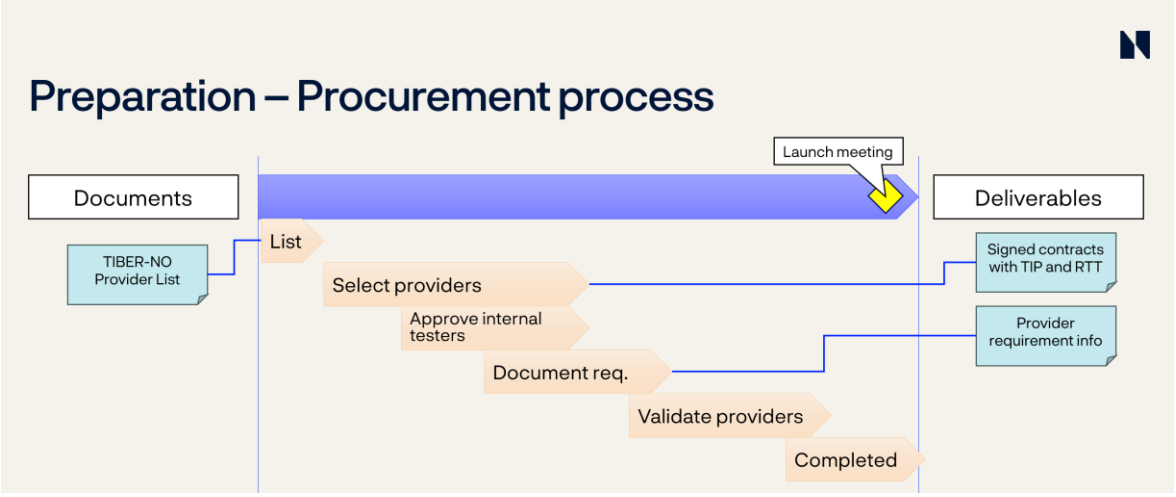
Responsible: CT
References:
- TIBER-EU 6.4
- RTS Art 9(6) and 9(7)
- Prop 54 LS (2024-2025)

The Scope Specification Document should be approved by the management body of the entity and informed to the TM within six months after receiving the written notification.

In context of Norwegian implementation of DORA, “Management body” can refer the entity’s board (“styre”) and executive manager (“daglig leder”). As the background for this approval is to accept and understand the scope and risks associated with the TIBER-NO test, the approval should be done by the board. (“styret normalt vil ha en «påse-plikt» mens daglig leder har det utførende ansvaret”).

If a third-party provider is included directly in the test, they too are expected to approve the scope. Any authorised signatory (“signaturrett” or “prokura”) at the third-party provider may approve the scope.

2.4 Procurement process



Owing to the sensitive nature of the TIBER-EU test, and since it is carried out on live production systems, the TIP and RTT shall possess the highest levels of skills, capabilities and qualifications. The entity must therefore select an external TIP and external (or under certain circumstances internal) RTT with the requisite skills and experience to perform the test.

Relevant documents for this process

- TIBER-EU Guidance for Service Provider Procurement (GSPP)
- TIBER-NO Provider List
- TIBER-NO Provider Information
- TIBER-NO Approval Checklists
- DORA Article 27: Requirements for testers for the carrying out of TLPT

Deliverables

- Signed contracts with TIP and RTT
- Provider Requirement information

2.4.1 List of providers

Responsible: TCT
References: TIBER-NO Provider List

TCT maintains a list of providers who have shown interest in offering threat intelligence or red-teaming services for TIBER-NO tests. This list can be supplied to the entity on request. The providers on the list are not vetted in any way by the TCT, and the entity may choose providers not on the list, as long as they fulfil the provider requirements for TIBER-NO tests.

2.4.2 Select providers

Responsible: CT
References:
- TIBER-EU 3.6.3, 4.1.3, 4.1.4 and 6.5
- TIBER-EU Guidance for Service Provider Procurement
- DORA Art. 26(8) and 27(1) to 27(3)
- RTS Art. 7, 15 and 9(11)

The entity evaluates if it wishes to use internal Red Teaming Testers (RTT) if they are permitted, see TIBER-EU 3.6.3. This shall only be done in exceptional circumstances and requires prior approval by the TCT. In such cases, internal testers need to adhere to the same standards and requirements as external RTT. Testers employed by an ICT intra-group service provider are considered as internal testers. If internal testers are used, external testers must be used every third test according to DORA. The Threat Intelligence Provider (TIP) shall always be external.

The entity evaluates possible providers of Threat Intelligence and Red-Teaming services for the TIBER test. This can be based on previous experiences with a provider or can be a more elaborate RFP process.

When procuring TIP and RTT, the CT 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.

To ensure the TIP and RTT meet the appropriate standards for conducting such a test, the entity should conduct its own evaluation as part of its procurement process and existing risk management practices to ensure the procured TIP and RTT meet the minimum requirements set out in the TIBER-EU Guidance for Service Provider Procurement. These are deliberately stringent requirements intended to mitigate the risk of tests being conducted by inexperienced personnel, which could have an adverse impact on the operational stability of the tested entity or the execution of the test.

Regarding the relevant certifications for the RTT and TIP, the providers send copies of certifications to the CT. Responsibility for ensuring the appropriate TIP and RTT are selected lies solely with the entity. The CT should document its assessment of compliance and provide evidence of compliance to the TM. The CT should not proceed with contracting the selected TIP or RTT until the Validation of providers is completed successfully by the TCT.

In exceptional circumstances, the entity could end up having to contract testers that do not meet the minimum requirements for providers. In such a case, the entity is required to adopt appropriate measures mitigating the risks relating to the lack of compliance with the requirements and provide evidence of these measures to the TM. If applicable, the above circumstances will be documented in the test attestation.

Once the procurement process has been completed and all relevant contractual arrangements are in place, the CTL should update the project plan in consultation with the TM, including the final schedule of process steps, deliverables and meetings to be held between the entity, TIP, RTT and TM. The CTL should share all relevant parts of the initiation documents, such as the project plan, secure communication and data exchange channels as well as the code name with all the relevant stakeholders.

The TM may allow a degree of flexibility to the entity on the timing of the procurement, as the process may differ across jurisdictions. However, the procurement of providers must be finalised before the start of the testing phase. The entity should, as early as possible, start the procurement process to ensure there are no bottlenecks or delays in the overall testing process.

2.4.3 Approve use of internal testers (if applicable)

If the entity expresses a desire to use internal testers, the TCT shall approve this prior to testing. The TCT should utilise the TIBER-NO Approval Checklists for Internal Testers for evaluation and should give written feedback to the CTL of the approval.

Responsible: TCT
References:
- TIBER-EU 3.6
- DORA Art. 27(2)
- RTS Art. 15(1) to 15(4)

Instead of using only internal testers, the recommendation is to have at least an experienced external RT test manager join the internal testers. This brings a fresh and independent perspective to the test, facilitates further development of the internal RTT, and provides additional experience with testing the entity's production system.

2.4.4 Document provider requirements

The CT compiles information about the providers documenting how they satisfy the requirements for a TIBER test. This can be references, individual team members' CVs, etc. Responsibility for ensuring the appropriate TIP and RTT are selected lies solely with the entity. The CT should document its assessment of compliance and provide evidence of compliance in the TIBER-NO Provider Information. The CT does not proceed with contracting the selected TIP or RTT when the TM assesses the selected providers do not ensure compliance.

Responsible: CT
References: TIBER-EU 6.5

This information shall be sent TM for validation.

2.4.5 Validate providers

Responsible: TCT
References:
- TIBER-EU 4.1.3 and 6.5
- TIBER-EU Guidance for Service Provider Procurement
- DORA Art. 26(8) and 27(1) to 27(3)
- RTS Art. 7, 9(11) and 15

The TCT ensures all minimum requirements are met, using the TIBER-NO Approval Checklists for providers. Where requirements are not met, or if insufficient documentation is provided by the CT to demonstrate how requirements are met, the TM shall contact the CTL to request further documentation. The TM can also suggest changes to the teams in order to satisfy the needed requirements.

In exceptional circumstances, such as when it is not possible for the CT to find a provider meeting the minimum requirements, the test can be allowed to proceed with extra risk reducing measures. The lack of meeting the minimum requirements shall be documented in the test attestation.

After the providers are successfully validated and complete, the TM should notify the CTL of its validation by written feedback.

2.4.6 Launch meeting

Responsible: CT
Participants: TCT, TIP, RTT
Type: Physical
Typical duration: 4 hours
Deadline: 6 months after written notification
References:
- TIBER-EU 6.5
- RTS Art. 9(8) and 9(9)

After the contracts with the TIP and the RTT have been signed, the CT organises a launch meeting to officially onboard the TIP and RTT to the test and to introduce them to the testing process, project plan, rules of engagement and stakeholder expectations. This meeting should include all relevant stakeholders who will actively be involved in the test. Physical participation is strongly encouraged, as this meeting is where all stakeholders can meet for the first time and gives a good way to get to know each other.

At the meeting, the TIP and the RTT are expected to present their teams and explain their methodology regarding the TIBER-NO assignment and the entity's test scope. The TIP and the RTT should outline how they expect to cooperate with each other during the test.

The launch meeting is held when the procurement is finalised, no later than six months after the written notification.

Agenda

- Presentation of participants
- TCT presents TIBER and expectations for participants
- Presentation of detailed project plan
- Scope Specification
- Presentation of TIP and methodology
- Presentation of RTT and methodology
- Rules of engagement and communication channels

Outcomes

- Agree on the project plan
- Establish a good basis for collaboration
- Align expectations

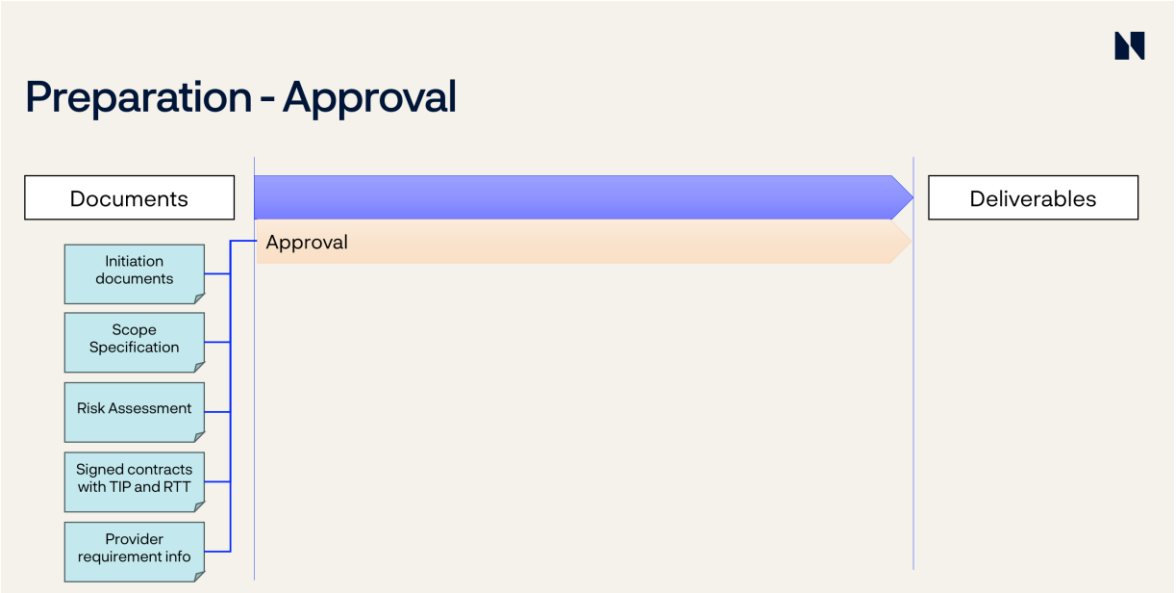
2.4.7 Procurement completed

The CT has completed procurement of the TIP and RTT and onboarded them to the test, prior to the start of the testing phase. The compliance of the providers with the applicable requirements and criteria has been assessed by the CT and TM.

Responsible: CT
References: TIBER-EU 6.5

2.5 Approval process

The final process of the preparation phase is to approve the documentation produced and ensure the TIBER test is ready to move on to the testing phases.



Relevant documents for this process

- Initiation documents
- Scope Specification Document
- Risk Management Documentation
- Signed contracts with TIP and RTT
- Provider Requirement information

2.5.1 Approval

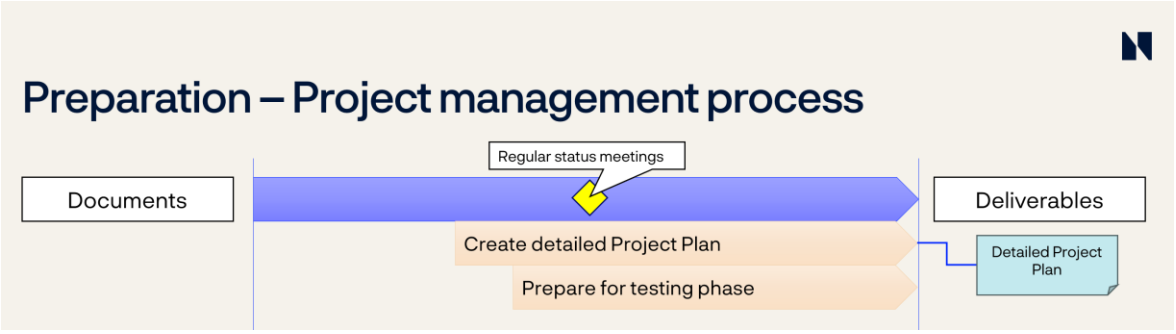
Responsible: TCT
References: TIBER-EU 7.2.2

The TCT shall approve the required preparations for the TIBER test are fulfilled. This includes:

- Initiation documents, based on previous validation (see 2.2.3)
- Scope Specification document and Risk Assessment documentation, based on previous validation (see 2.3.6)
- Providers of TIP and RTT based on previous validation (see 2.4.3 and 2.4.5)

The approval shall be communicated to the CT, marking the completion of the preparation phase of the test.

2.6 Project management process



During the entire TIBER test, there are many processes and activities to keep track of, and it can be challenging to keep the overview at all times. To run the project smoothly, a separate project management process is included for all phases. This is to emphasise the importance of well-structured management throughout the project, and to give recommendations on how to run the project efficient and smoothly. The CTL is responsible for the project management during the test, if no other specific resource is appointed within the CT.

Relevant documents for this process

- Initiation documents
- Risk Management Documentation

2.6.1 Create detailed Project Plan

Responsible: CTL
References: TIBER-EU 6.5

As early as possible, the CTL should begin developing a detailed project plan. The entity should use its own format for the detailed project plan, but the content of the plan should be based on the TIBER-NO Test Overview (Excel) and the dates agreed between the entity and the TCT.

The detailed project plan must include a schedule of meetings to be held between the CT, TIP, RTT and TCT as well as a schedule for other activities, including input collection to deliverables, review and approval processes, delivery of the planned deliverables in draft and final draft versions, and internal communication.

Once the TIP and RTT are in place in the preparation phase, the CT shall have a complete detailed project plan for the launch meeting. The detailed project plan shall be updated continuously throughout the test and any deviations from the original planning should be discussed in advance with the TCT.

2.6.2 Prepare for testing phase

Responsible: CT
References: TIBER-EU 7.2.1 and 7.2.2

TIBER is designed to create realistic threat scenarios describing attacks against an entity's critical and important functions. Real-world threat actors may have months to prepare an attack. Hence, to make intelligence gathering as efficient as possible given time and resource constraints, the TIP should be provided with relevant information that might help their analysis. The entity should ensure this is only information which could be found with enough time and resources to make the process more efficient and add value.

Some examples of the information that can be provided:

- A business and technical overview of each CIF -supporting system in the scope
- The current threat assessment and/or threat register
- Examples of recent attacks on the entity or its environment
- Previous TTIR used in TIBER tests, if relevant and deemed feasible by the entity

Obtaining the relevant input for the TIP without alerting the organisation of an imminent test may require the CT 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 TIP is signed.

The TIP may start preparations for the threat intelligence phase, for instance agreeing on a detailed time schedule for the phase in line with the Initiation Documents. If relevant, the TI Provider should give input to the scope and risk management.

The RTT should start preparations for the red-teaming phase, for instance agreeing on a detailed time schedule for the phase in line with the Initiation Documents. If relevant, the RTT should give input to the scope and risk management, for instance regarding rules of engagement.

2.6.3 Regular status meetings

Throughout the preparation phase, there should be regular status meetings between the CT and the TCT to ensure continued progress of the planning process for the test.

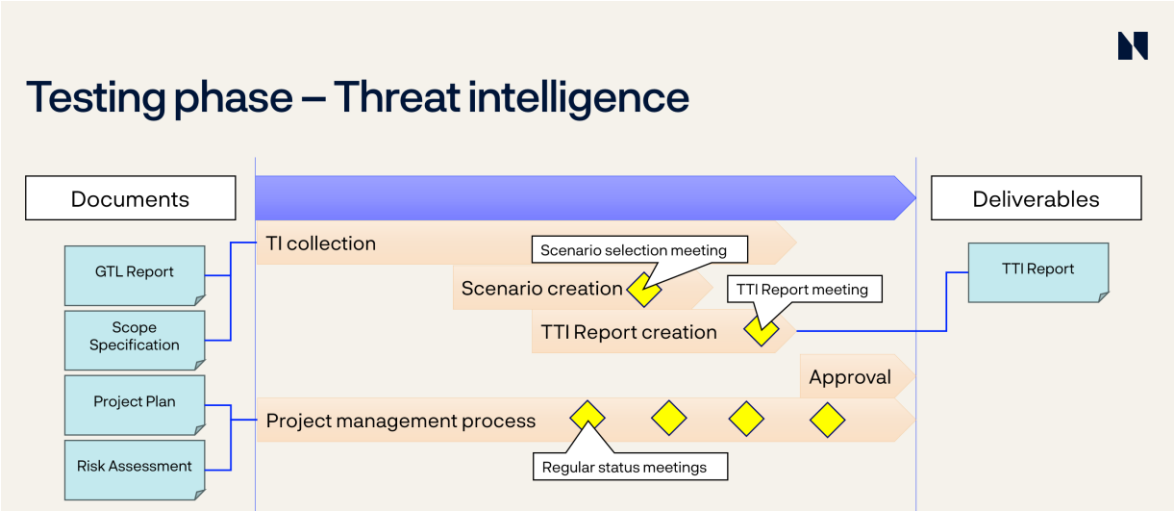
The meetings can be held each week or each second week, depending on the needs of the CT and how quickly the test planning progresses.

Responsible: CT
Participants: TCT
Type: Online
Typical duration: 30 minutes
References: None

Agenda

- Current status of planning
- Outstanding questions
- Project plan follow-up

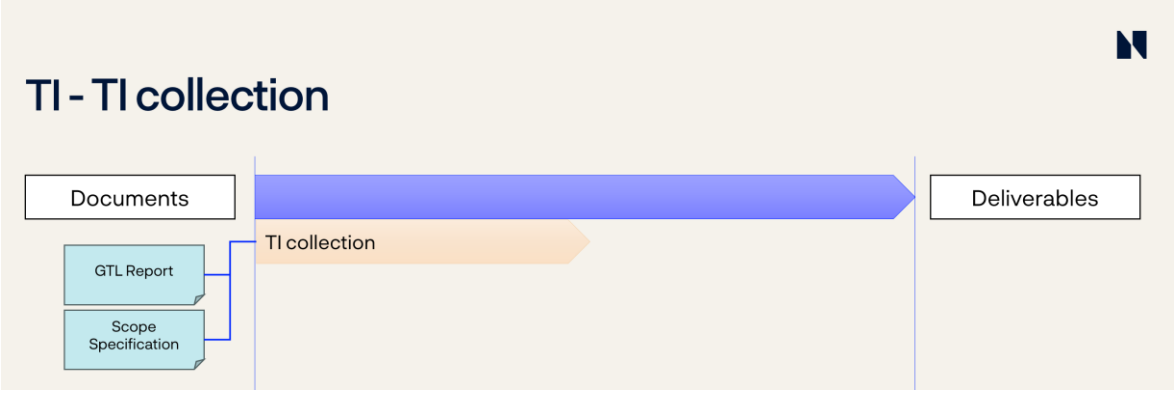
3 Testing phase: Threat intelligence



Once the preparation phase with all its activities is finalized, the testing phase officially begins. The testing phase starts with the threat intelligence (TI) component which is the passive reconnaissance stage of the TIBER-NO test. This phase is estimated to span over at least 4-6 weeks in addition to the approval process.

The threat intelligence phase further consists of three processes: TI collection, scenario creation, and Targeted Threat Intelligence Report (TTIR) creation. The approval process and project management processes come in addition. The main delivery from this phase is the TIBER-NO Targeted Threat Intelligence Report on the entity, setting out threat scenarios for the test and useful information on the entity.

3.1 Threat intelligence collection process



For the TIBER-NO framework to work effectively, the TTI process and subsequent deliverables shall meet the highest standards. Intelligence encompasses not only the technical details of the attack but also an understanding of the tactics, techniques, and procedures (TTPs) behind the attack and the threat actors themselves, including their intent, capability and modus operandi.

The TI provider is expected to:

- Engage with the entity to obtain useful context for conducting the threat analysis

- Use a broad range of sources, e.g. internet services, a mixture of public and private forums and a range of media types such as internet relay chats, email and video
- Have a depth of sources. I.e. the TI provider can look up original sources and not just rely on surface content
- Only use TI gathering techniques that do not risk compromising the secrecy of the test
- Have adequate language support, particularly for Norwegian language and languages used by Norway's major adversaries
- Be able to use a variety of methods in intelligence gathering
- Demonstrate strong ethical behaviour
- Cooperate with the RTT in a flexible and transparent manner, when required, in the testing process

The Control Team is expected to provide a business overview with known threat intelligence information, both publicly available information and other relevant information known to the entity, see section 2.6.2. Together with intelligence from the Generic Threat Landscape (GTL) Report, the TI Provider should focus on collecting, structuring and analysing targeted information on the entity and CIFs not already known to the entity.

Relevant documents for this process:

- TIBER-NO Generic Threat Landscape Report
- Scope Specification Document
- TIBER-EU Targeted Threat Intelligence Report Guidance
- TIBER-NO Targeted Threat Intelligence Report Guidance

3.1.1 Threat intelligence collection

Responsible: TIP
References:
- TIBER-EU 7.2
- RTS Art. 10(1)

During the TI collection, the TIP 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 phase is strictly passive, and no active reconnaissance should be undertaken by the TI provider. 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, 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

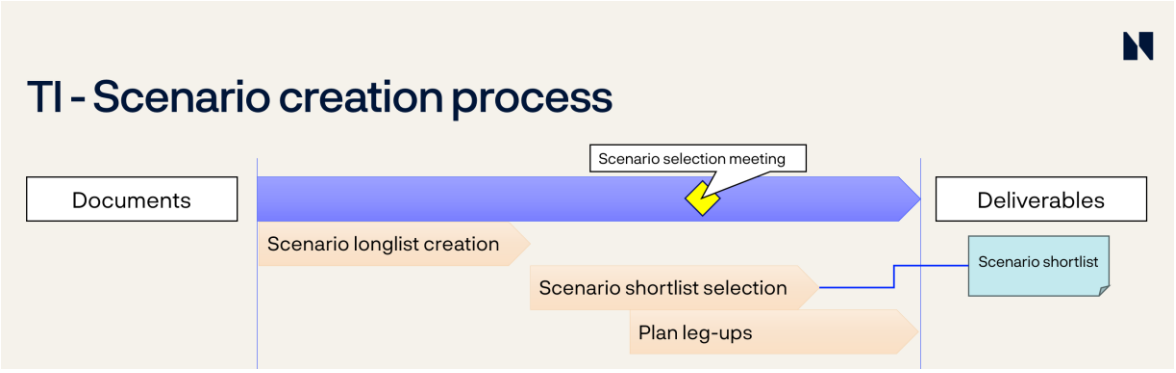
the entity and its digital footprint. This includes information intentionally published by the entity and internal information that has been unintentionally leaked.

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.

3.2 Scenario creation process



Relevant documents for this process

- TIBER-NO Generic Threat Landscape Report
- Scope Specification Document
- TIBER-EU Targeted Threat Intelligence Report Guidance
- TIBER-NO Targeted Threat Intelligence Report Guidance

Deliverables

- Scenario Shortlist

The scenarios chosen for the TIBER test shall be based specifically on the collected Threat Intelligence information for the entity. The “targeted” TI shall be interpreted as specific to the entity, not the sector, country or other more generic interpretations.

One of the selected scenarios may be non-threat-led and may be based on a forward-looking threat, with high predictive, anticipative, opportunistic or prospective value. Such scenarios are also known as ‘scenario X’ and may include hybrid, novel TTPs and “out of the box” elements. The scenario X should be based on anticipated developments of the threat landscape customised to the entity. See the TIBER-NO Targeted Threat Intelligence Report Guidance for further details of using Scenario X.

The TIP should provide further input on the flags set by the CT in the Scope document, based on the information and knowledge they acquire about both the entity and relevant threat actors through their work.

3.2.1 Scenario longlist creation

Responsible: TIP
References:
- TIBER-EU 7.3
- RTS Art. 10(2) to 10(4)

Equipped with the output from the target identification and threat identification, the TIP should create a broad set of scenarios, called a scenario longlist, which should be presented to the stakeholders in the scenario selection meeting. The scenario longlist should typically consist of at least 6 to 10 suggested scenarios. The scenarios should be high-level, tailored to the tested entity, vary regarding the included threat actors and TTPs, and cover all CIFs which are in scope. Based on the scenario longlist, the final scenarios used for testing will be selected and elaborated in more detail in the TTIR.

3.2.2 Scenario selection meeting

Responsible: CT
Participants: CT, TCT, TIP, (RTT)
Type: Physical or virtual
Typical duration: 2 hours
References: TIBER-EU 7.3

A scenario selection meeting is held when the longlist of scenarios is ready to be shared and discussed. The longlist should be distributed to the participants one week prior to the meeting to ensure all meeting participants are well prepared.

The TIP explains the background for each threat scenario in draft, and together the participants evaluate the longlist and narrow it down to the three most relevant threat scenarios. More scenarios could be specified as well, but TCT-NO recommends keeping the number of scenarios to three.

Preparation

- TIP shares scenario longlist it with other participants 1 week prior to the meeting
- All participants prepare input to the scenarios

Agenda

- Presentation of Scenario Longlist including background, methodology, threat actors, TTPs and CIFs
- Suggestions for adaption
- Alignment on selection of scenarios

Outcomes

- Draft threat scenarios presented by TIP and discussed by participants
- Alignment on a minimum of three scenarios to be selected or adapted

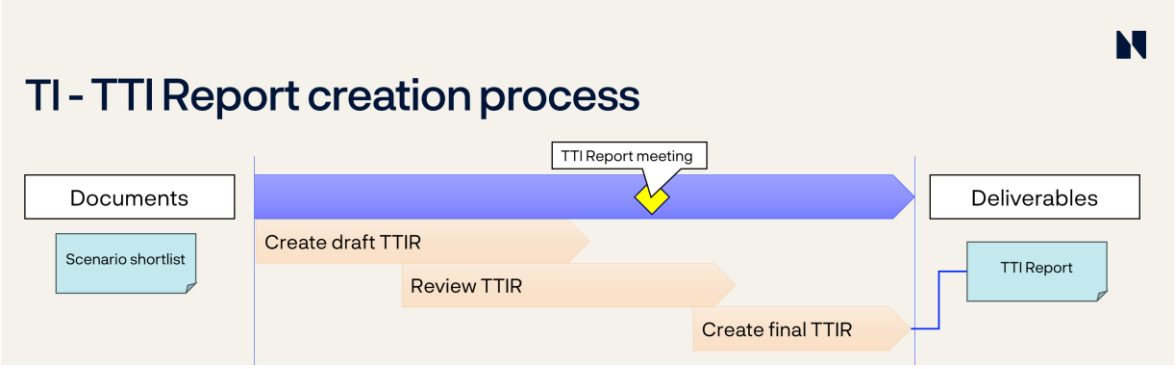
3.2.3 Scenario shortlist selection

Responsible: CT
References:
- TIBER-EU 7.3
- RTS Art. 10(3) and 10(4)

After the scenario selection meeting, the CTL should have the final word on which scenarios that should be selected.

The CTL selects/adapts three or more scenarios to be followed during testing, based on the requirements in TIBER-EU Targeted Threat Intelligence Report Guidance. These should be documented in a deliverable, “scenario shortlist”. There are no further requirements for the format or content of the shortlist. Hence it could be in an optional format, e.g. meeting minutes, power point etc. The deliverable does not need any specific approval from the TM, but it should be shared with the TM to document how the scenarios will meet the requirements later stated for the TTIR.

3.3 TTI Report creation process



Relevant documents for this process

- TIBER-EU Targeted Threat Intelligence Report Guidance
- TIBER-NO Targeted Threat Intelligence Report Guidance
- Scope Specification Document
- Scenario Shortlist

Deliverables

- Targeted Threat Intelligence Report

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 RTT in their attempt to capture the flags agreed upon in the scoping activity
- Validated evidence to support the business case for post-test remediation and improvement

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

Once the TIP has completed the Targeted TI Report, it should be shared with the CT, the TCT and the RTT in a draft version at least one week before the TTI Report meeting.

After the TIP has delivered its report and proposed adjustments to the flags, the CT may choose to adjust or change the flags they find appropriate. These updates are then reflected in the Scope Specification Document.

3.3.1 Create draft Targeted TI Report

Based on the threat intelligence collection process and the scenario creation process, the TIP shall compile all the information into a draft TTIR.

The report shall contain at least the elements detailed in:

Responsible: TIP
References:
- TIBER-EU 7.4
- RTS Art. 10(5)

- TIBER-EU 7.4
- TIBER-EU Targeted Threat Intelligence Report Guidance

The TTIR should be a standalone delivery and give value to the CT on its own. Information which is not included further in the TIBER test could be followed up by the CT on the later stage and hence give more value than just under the TIBER test itself.

The TIP should use terminology consistent with the TIBER guides wherever possible.

3.3.2 Review Targeted TI Report

When a draft is ready for reviewing, it is handed over to the CT and TCT.

Responsible: CT
References:
- TIBER-EU 7.4
- RTS Art. 10(5) and Annex III

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

The actionable data to be used by the RTT, e.g., the digital footprint of the entity, should be verified by the CT to not pursue non-existent possibilities in the red-teaming phase.

Any updated versions of the report should clearly highlight what changes have been made from previous versions to help the TCT and TCT review the updated version.

3.3.3 TTI Report meeting

All stakeholders should provide feedback on and discuss the report, identifying potential aspects to be added/changed. If necessary, flags might be updated in the light of the report data, and potential leg-ups should be explained. The TTIR meeting is held as soon as the report is in its final stage.

Responsible: CT
Participants: TCT, TIP, RTT
Type: Physical or virtual
Typical duration: 2 hours
References: TIBER-EU 7.4

The Red Team Testers should also be invited to this meeting to get an introduction to the report and to be able to ask questions regarding its contents and the suggested scenarios in the scenario shortlist.

Preparation:

- All participants should have read through the TTIR which should be delivered one week before the meeting

Agenda:

- The collected target intelligence
- The selected and detailed scenarios for testing
- The draft TTIR

Outcomes:

- Feedback on TTIR

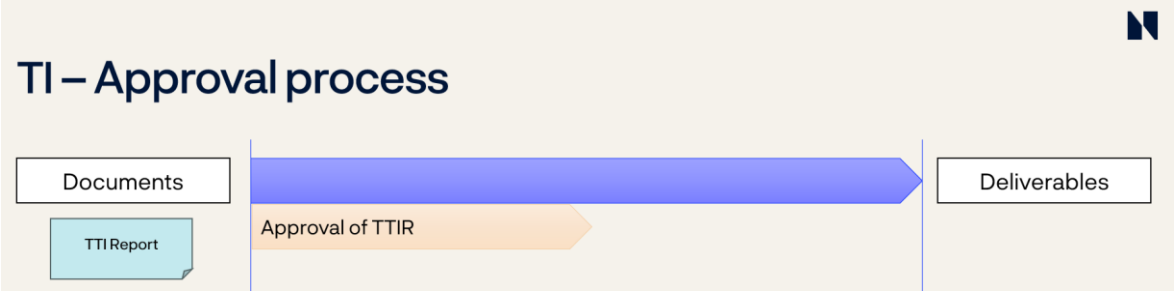
3.3.4 Final TTIR

Following the TTI Report meeting, the TIP should update the draft TTIR based on the received feedback. A completed version of the report shall be sent to the CT. If the CT is satisfied with the contents, the TTIR shall be forwarded to the TCT for approval.

Responsible: TIP, CT
References:

- TIBER-EU 7.4
- RTS Art. 10(6)

3.4 Approval process



Relevant documents for this process

- Draft Targeted Threat Intelligence Report

Deliverables

- Targeted Threat Intelligence Report

3.4.1 Approval of TTIR

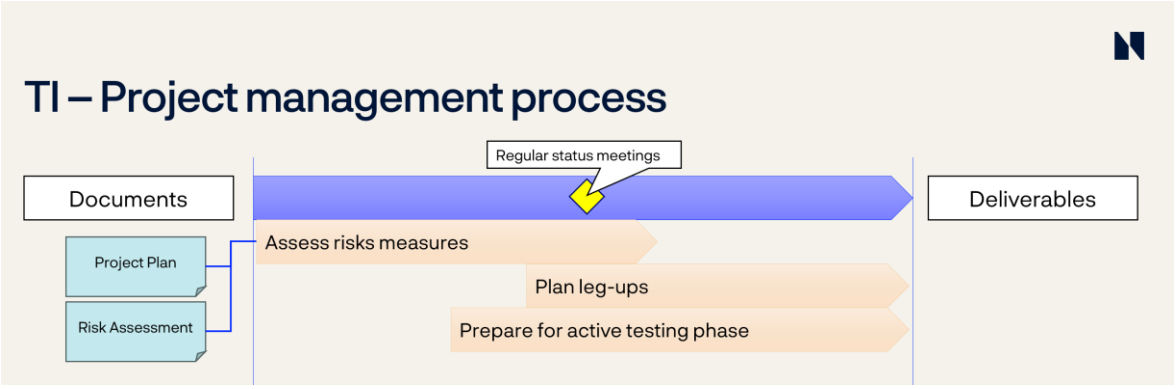
After finalisation, the CT should send the TTI report to the TM for approval.

The TM shall check the contents of the report towards the TIBER-NO Approval Checklists for TTIR. After the TTIR is successfully approved and complete, the TM should notify the CT Lead of its approval by written feedback.

Responsible: TCT
References:

- TIBER-EU 7.4
- RTS Art. 10(6)

3.5 Project management process



Relevant documents for this process

- Initiation documents
- Risk Management Documentation

3.5.1 Assess risk management measures

Responsible: CT
References: TIBER-EU 7.4

The CT should update their risk management controls after receiving the TTI Report.

The detailed scenarios chosen for the test will give more details to what will be tested in practice. A risk management assessment should be conducted to identify any further mitigating or risk reducing measures needed.

This can be done by updating the risk management documentation produced in the preparation phase of the test.

3.5.2 Plan and organise leg-ups

Responsible: CT
References: TIBER-EU 7.3

Based on the information of the collected TI and the selected scenarios, the CT must start to plan for the potential use of leg-ups. Leg-ups are network and system accesses and/or devices that may be needed by the RTT in their execution of the scenarios. Leg-ups could also include additional information on target systems and technology. The RTT are invited to offer their expert view on what kind of leg-ups would be more suitable. Actions such as directly providing access to the flags and/or disabling security controls should not be proposed as leg-ups.

The CT should start preparing leg-ups as early as possible to build credibility on leg-up assets such as accounts, computers and servers. This will make it more difficult to deduce a detected scenario as testing activity.

3.5.3 Prepare for active testing phase

Responsible: CT
References: TIBER-EU

The CT should prepare for the active phase throughout the TI phase. This can include, but is not limited to, review the flags set in scope, prepare leg-ups to be used in the testing, inform relevant actors,

make up cover stories for the blue team if suspicion is made. Also, it should be planned for de-escalation and made sure the correct persons and roles are included in the control team to stop escalation beyond the entity itself.

3.5.4 Regular status meeting

The CT, TCT and the TIP should schedule regular status meetings to ensure progress and alignment on the threat scenarios. Weekly meetings is often a good frequency for these status meetings.

Responsible: CT
Participants: TIP, TCT
Type: Online
Duration: 30 minutes
References: None

The CT and TCT should also consider if there is a need to give some informational leg-ups to the TIP during this phase to ensure there is good progression in the work of the TIP.

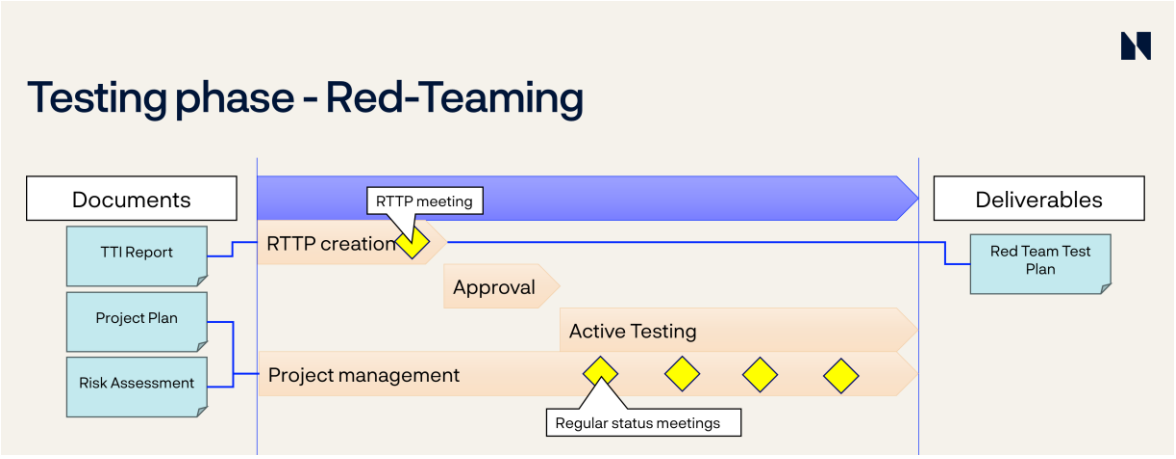
Agenda:

- Current status of TI
- Outstanding questions
- Project plan follow-up

Outcomes:

- Feedback on work and progress

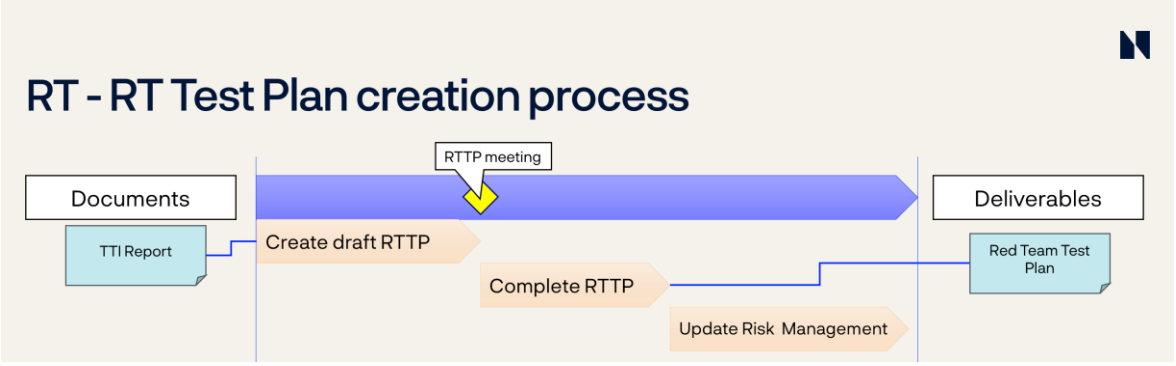
4 Testing phase: Red-Teaming



During the red-teaming phase, the RTT plans and executes a TIBER test based on the respective selected scenarios for the target systems and services supporting the selected CIFs in scope.

The time allocated for testing should be proportionate to the scope. The minimum time spent on active testing must be 12 weeks according to DORA RTS. Based on experience it is envisaged at least a total of 16 weeks (four weeks of preparation and 12 weeks of active testing) as a reasonable amount of time for the red-teaming testing phase.

4.1 RT test plan creation process



In this process step, the RTT develops and integrates the attack scenarios into a Red Team Test Plan (RTTP), leveraging on the scenarios included in the TTIR.

The RTT should align its test objectives with the goals of each of the actors, map these to the CIF-supporting systems, 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 to conduct a successful attack. The RTT should therefore adapt its attack methodology to replicate the real-life attack scenarios.

The output of this process is the final RTTP, including the attack scenarios to be followed and the risk management controls that will be applied to ensure the test is conducted in a controlled manner, including the frequency of test progress reports with the CT and the TM.

Flags shall be included in the RTTP and the RTT is given the opportunity to propose changes where they consider it relevant. After the RTT has proposed any adjustments, the CT is encouraged to re-assess the flags and, if changes are adopted, update them in the Scope Specification Document.

Relevant documents for this process:

- Scope Specification Document
- TIBER-NO Generic Threat Landscape Report
- Targeted Threat Intelligence Report
- TIBER-EU Red Team Test Plan Guidance
- TIBER-NO Red Team Test Plan Guidance
- TIBER-NO Leg-up Guidance

Deliverables:

- Red Team Test Plan

4.1.1 Create draft Red Team Test Plan

Responsible: RTT
References:

- TIBER-EU 8.3
- RTS Art. 11(1) and Annex IV

The RTT creates a draft RTTP based on the intelligence-led attack scenarios outlined in the TTIR. The plan can be based on the outline in the TIBER-NO Red Team Test Plan Guidance. The Red Team Test Plan may deviate from the TTIR and the proposed TTPs described, ensuring the intensions and motivations of the TA are intact. Such deviations should be described, including reasoning for the change.

The RTT 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.

Scenarios to be tested may also include the usage of TTPs which look to breach the physical security of the entity to gain access to the network or plant a device. However, if such a method is used, appropriate safeguards (e.g. formal consent by the entity) should be in place and no legal boundaries should be crossed.

It is advised the CT arrange status meetings with the RTT, the TCT and optionally the TIP during the development of the RTTP to ensure progress and alignment with the scope, the threat intelligence, and the overall expectations of the attack plan.

The RTT should use terminology consistent with the TIBER guides wherever possible.

4.1.2 Red Team Test Plan meeting

Once the RTTP is in its final phase, the RTT, TM, CT, and the TIP, where appropriate, come together to discuss it during the RTTP meeting. The RTT explain their envisioned approach to reach the flags, as well as the technical measures they will take for doing so, and the leg-ups they might require at certain points.

Responsible: CT
Participants: RTT, (TIP), TCT
Type: Physical or virtual
Typical duration: 2 hours
References:
- TIBER-EU 8.3
- RTS Art. 11(2)

Preparation:

- Distribute draft RTTP at least 3 working days in advance

Agenda:

- RTT presents draft RTTP
- Feedback on RTTP

Outcomes:

- Updates to draft RTTP to be amended in the final RTTP

During the RTTP meeting the RTT should present:

- Planned attack steps for each end-to-end scenario, including detailed flags and expected leg-ups
- Time planning for each scenario
- Dedicated milestones
- Escalation contacts and procedures
- Rules of engagement and reporting agreements
- Risk management measures taken by the RTT

4.1.3 Complete final Red Team Test Plan

Based on feedback from the CT, TIP and TCT in the RTTP meeting, the RTT update the Red Team Test Plan to a final version ready for approval.

Responsible: RTT
References: TIBER-EU 8.3

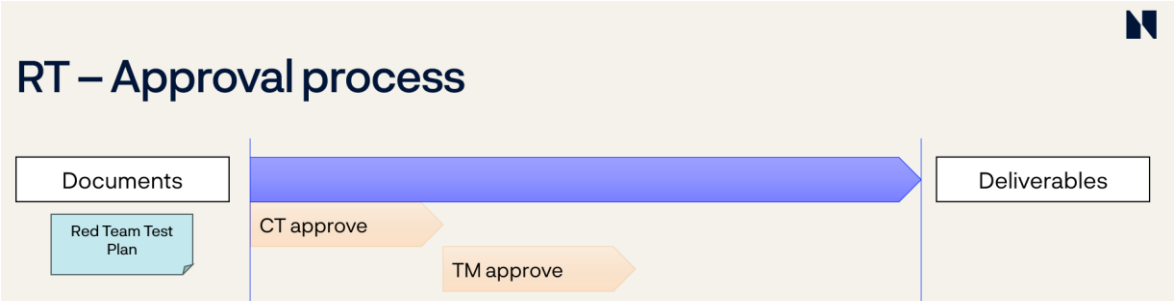
The final RTTP is distributed to the CT and TCT.

4.1.4 Update Risk Management controls

Upon finalisation of the RTTP, the CT must update its risk management controls and prepare specific leg-ups for the RTT, by being ready to execute all necessary processes and procedures without raising alarm and causing delay.

Responsible: CT
References: TIBER-EU 8.3

4.2 Approval process



The CT and TM shall approve the final RTTP after the draft RTTP has been updated following the RTTP meeting.

Any changes to the RTTP following its approval must be approved again by the CT and TM.

A successful approval marks the formal start of the active testing.

Relevant documents for this process:

- Red Team Test Plan
- TIBER-NO Approval Checklists

4.2.1 CT approves final RTTP

Following the finalisation of the Red Team Test Report, the CT shall approve contents of the report, thereby accepting the planned attacks and the associated risks.

After the RTTP is approved, the CT should notify the TM.

Responsible: CT
References:

- TIBER-EU 8.3
- RTS Art. 11(3)

4.2.2 TM approves final RTTP

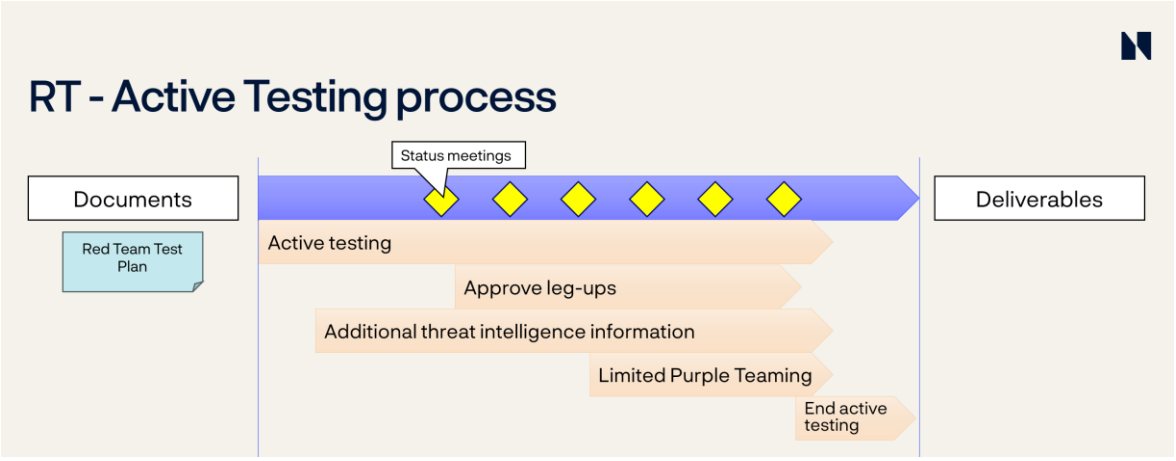
The TM gives an approval of the delivered final RTTP, ensuring the minimum requirements are met following the TIBER-NO Approval Checklists for RTTP and the plan covers the spirit and intensions of the TIBER-NO test.

Responsible: TCT
References:

- TIBER-EU 8.3
- RTS Art. 11(3)

After the RTTP is successfully approved, the TM should notify the CTL of its validation by written feedback.

4.3 Active Testing process



The attack scenarios are not a prescriptive playbook which must be followed precisely during the test. If obstacles occur, the RTT should show its creativity (as advanced attackers would) to develop alternative ways to reach the test objective or flag.

A minimum of 12 weeks must be allocated to active testing, to allow the RTT to conduct a realistic and comprehensive test in which all attack phases are executed within this time frame, attack scenarios can be executed in parallel or in sequence. When executing scenarios in parallel, the RTT still needs to complete all the scenarios' IN, THROUGH and OUT phases.

The RTT is constrained by the time and resources available as well as by moral, ethical and legal boundaries. Therefore, RTT may require occasional leg-ups in addition to those laid out in the test plan to help the RTT progress. All leg-ups are to be provided by the CT and approved by both the CT and the TM.

As input to the activities in the closure phase, it would be beneficial for the CT to keep a log of the attack seen from their point of view and a log of their own actions. Ideas for activities in the purple team exercise in the closure phase should also be written down as they encounter.

During the execution of the test, it can happen a staff member of the entity or its ICT third-party service provider irrevocably detects the RTT via its activities. In such cases, the CT should propose and submit measures allowing to continue the test to the TM for its validation whilst ensuring the secrecy of the test is upheld. Other cases may include the discovery of an actual compromise or any other exceptional circumstances triggering risks of impact on data, damage to assets, disruption to CIFs, services or operations. Under such exceptional circumstances, after consultation with the TM, the CTL may suspend the test as needed to thereby facilitate delays or employ other changes to continue the test and maximise its learning experience.

In case a critical vulnerability is discovered during this phase, the CT may also initiate remediation actions, based on technical feedback provided by the RTT, and in close consultation with the TM, while ensuring the minimum possible impact to the testing activities and confidentiality.

Irrespective of the methodology used by the RTT, the test should be conducted in a controlled manner, taking a stage-by-stage approach to minimise any risks to the entity

and its CIFs. All of the RTT actions should be logged: for the later replay exercise with the BT, as evidence for the RTTR, and for future reference.

Relevant documents for this process:

- Red Team Test Plan
- TIBER-NO Leg-up Guidance
- TIBER-NO Red Team Status Reporting (PowerPoint)

4.3.1 Active testing

Responsible: RTT
References:
- TIBER-EU 8.4
- RTS Art. 11(5), 11(6), 11(8) and 11(9)

The active testing activity starts with RT starting to execute one or more of the scenarios.

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.

If there are changes to the RTTP during the active testing phase, the CT and TM shall approve the changes.

Leg-ups proposed when needed and when it gives value in the scenario. However, before being used, the TM and CT must approve it.

If test activities are detected by any member of the blue team, the CT shall propose measures to allow the test to continue without revealing it to all. This shall be validated by the TM.

4.3.2 Weekly status meetings

Responsible: CT
Participants: TM, RTT, (TIP)
Type: Physical or Online
Typical duration: 30 minutes
References:
- TIBER-EU 8.4
- RTS Art. 11(7)

During active testing, the CT shall organise at least weekly meetings for the RTT to update the CT and TM on the testing progress. For example, the activities conducted in the past week along with activities expected in the upcoming week. The TIP may be involved for consultation if requested by the CT.

In addition to the weekly updates, RTT should arrange short daily meetings and ad-hoc (secure) communication involving the CT and the TM. The focus should be on activities of the immediate past and short-term planned actions, especially during critical testing phases. The weekly status meetings should still cover the previous week's activities to ensure everyone is kept up to date on all activities.

Agenda:

- RTT presents the current status
- RTT presents planned activities coming days
- Other coordination and needs, such as leg-ups etc.

Outcomes:

- Short written status

As an example of reporting template, see the TIBER-NO Red Team Status Reporting (PowerPoint).

The RTT can consider someone else than the Lead to facilitate the status meetings to let the Lead focus on the testing activities and not spend valuable time organising the meetings.

4.3.3 Submit leg-ups

Responsible: CT
References:

- TIBER-EU 8.2.2
- DORA RTS Art. 11(8)

There will likely be situations where RTT will need assistance to proceed with a scenario. A real attacker will have ample time and resources not normally available during the TIBER test. To compensate for this while retaining realism in the test, the RTT can be provided with leg-ups to progress.

It is recommended to provide as little help as feasible to not help the RTT unreasonably much. In practice, this means for instance providing informational information over access to systems. Leg-ups should be specific to one scenario. The use of the same leg-up in different scenarios is discouraged.

The leg-up shall be described with the following details:

- An identifier – such as LU-[scenario-letter]-[number]. Example: LU-A-01 for scenario A.
- Short description
- Type – information, access or assistance, or a combination of these.
- Which scenario the leg-up is for
- Reason – such as time saving, ethical or resource saving
- What the leg-up compensates for
- Any prerequisite to activate the leg-up
- Date requested

All leg-ups shall be documented and time of activation logged.

See the TIBER-NO Leg-up Guidance for further details on preparing leg-ups.

4.3.4 Approve leg-ups

Upon receiving a request for a leg-up, the TM shall ensure all necessary information regarding the leg-up is provided by the CT. The TM shall then evaluate if the leg-up is appropriate for the scenario and gives the best possible value for the test.

Responsible: TCT
References:
- TIBER-EU 8.2.2
- DORA RTS Art. 11(8)

The CT and TM are required to approve each leg-up before it is given to the RTT.

4.3.5 Additional threat intelligence information

The TIP can cooperate with the RTT during the remainder of the TIBER-NO test. This includes helping to update the attack scenarios if needed, as well as any new intelligence requirements that occur as the Red Team test progresses. The TIP is expected to provide input into the final report issued to the entity.

Responsible: TIP
References:
- TIBER-EU 8.2.2

4.3.6 Information to Blue Team

When the Blue Team suspect they are being tested, planned and good cover stories can help. If this is not sufficient, consider informing there is test ongoing without informing it is a TIBER test, since this involves multiple scenarios.

Responsible: CT

When the Blue Team are informed of the full TIBER-test, they do not have the same background as members of the CT. To get an understanding of the test, consider giving them access to documents such as Scope Specification Document, GTL, TTIR, RTTP, TIBER-NO documentation and the BTTR guidance.

As this can be a large amount of information at once, consider also a briefing from the CT or TIP.

4.3.7 Limited Purple Teaming (optional)

As a last resort, if continuation of the test is not otherwise possible, and as far as possible strictly within a scenario, testing activities can be continued as a limited purple teaming exercise during the active testing phase, subject to prior validation of the TM.

Responsible: RTT
References:
- TIBER-EU 8.4
- RTS Art. 11(10)

The CT can also consider if other parties could be involved in the Limited Purple Teaming activity, such as for instance NFCERT.

The duration of the limited PT exercise counts towards the 12-week minimum duration of the active testing phase. This limited purple teaming focuses on performing the rest of the scenarios set out in the RTTP which have not yet been covered. New scenarios should be considered for the purple teaming in the closure phase instead, if relevant.

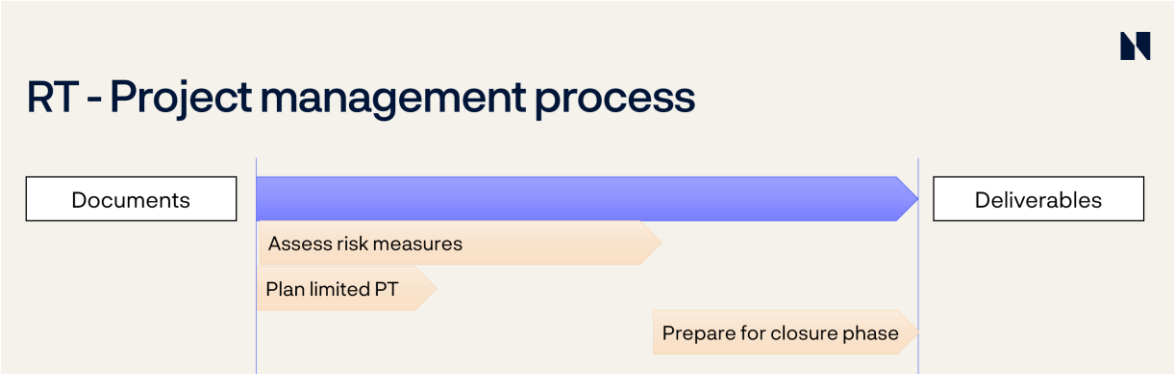
4.3.8 End active testing

The CT, TIP, RTT and TM should agree on the concrete end of the active red-teaming phase. Following the end of the active red-teaming phase, the CTL will inform the BT a test was conducted.

Responsible: CT
References: TIBER-EU 8.4

Restoration activities can be performed as described in 5.3.2, if deemed appropriate.

4.4 Project management process



Regular status meetings must be arranged in this phase too, but they are included in the Active Testing process. Additional project management status meetings may be held in addition.

Relevant documents for this process:

- Risk Management Documentation
- TIBER-EU Purple Teaming Guidance

Deliverables:

- Updated Initiation documents

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

4.4.1 Assess risk measures

CT should update their risk management controls throughout the whole active testing phase. Particularly, risk management controls should be considered thoroughly when the Red Team Test Plan is developed to ensure sufficient risk measures are in place during the active testing period.

Responsible: CT
References: TIBER-EU 7.2.2

The risk management documentation can be further updated to reflect the identified risks and possible mitigating and risk reducing measures implemented.

4.4.2 Plan Limited Purple Teaming

Responsible: CT
References: TIBER-EU 8.4

Planning for the limited purple teaming should be done at an early stage in the active testing, as moving to this activity can be needed very quickly. Understanding the various options here in advance will enhance the learning experience from the limited purple teaming. See the TIBER-EU Purple Teaming Guidance document for available options for Purple Teaming in the active testing phase.

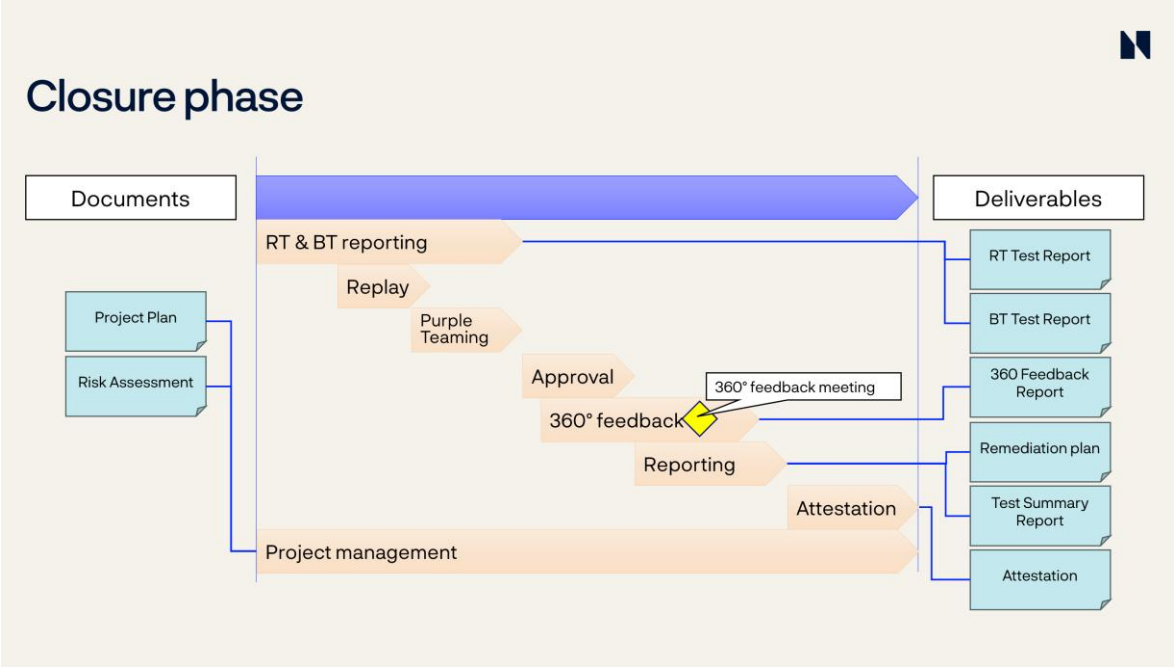
How members of the Blue Team should be informed and onboarded should be prepared. Ensure also the Blue Team have resources and capacity to collaborate during this limited purple teaming period.

4.4.3 Prepare for closure phase

Responsible: CT
References: None

When the active testing activities are coming to an end, preparing for the closure phase can be done. This should include organising and preparing for the report writing for the RTT and blue team.

5 Closure phase

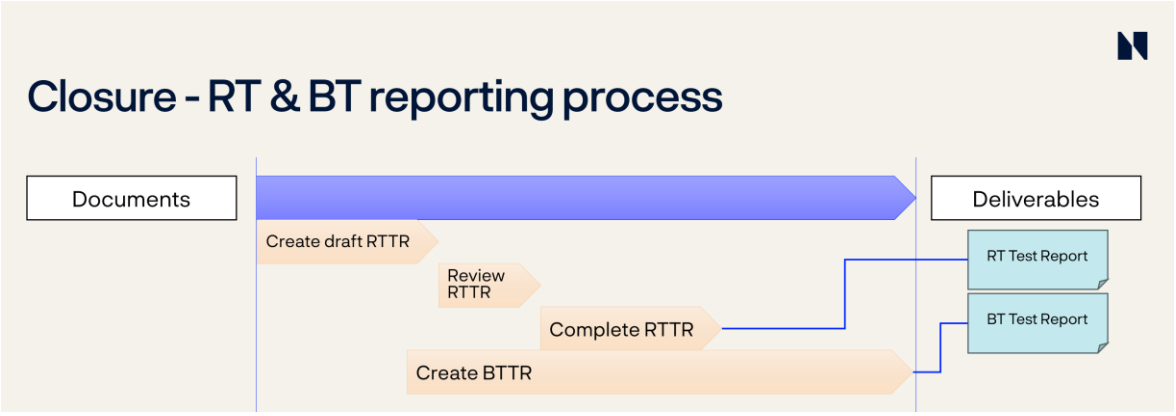


The closure phase allows all relevant stakeholders to reflect on the outcome of the test and make improvements to further enhance the cyber resilience of the entity. Once the active testing is concluded and the Blue Team (BT) has been informed about the test, the RTT and the BT start to create their respective test reports. The Red Team Test Report (RTTR) includes details of the approach taken to the testing and the findings and observations from the test, whereas the BT Test Report (BTTR) includes details on the observations of the BT during the test, mapped alongside the actions of the RTT.

Once these reports are in a final stage, the replay process commences, followed by the Purple Teaming (PT) process step. After the replay and PT process steps, the CT finalises the test summary report and remediation plan. When the PT step has concluded, the 360°-feedback process step commences, during which all relevant stakeholders deliver feedback on each other, and the overall testing process. The test is concluded with the attestation process where the TIBER authority formally approves the test.

The first part of the closure phase, containing the writing of the RTTR and BTTR and the replay and PT exercises, takes a maximum of 10 weeks. The second part of the closure phase relates to the TM's assessment of the BTTR and the RTTR. The third part of the closure phase, related to the 360° feedback and the writing of the test summary report and the remediation plan, takes a maximum of 8 weeks. Finally, the closure phase ends with the test attestation. Depending on the time the TM needs for the assessment of the RTTR and BTTR and for the attestation, the total duration of the phase may be longer than 18 weeks.

5.1 RT & BT reporting process



These process steps commence after the active testing has been concluded and the key members of the entity's BT are informed about the test. The RTT produces a RTTR, for delivery to the CT within four weeks from the end of the active red team testing phase, which in turn delivers it to the BT and the TM. It is then used by the BT to deliver the BTTR, no later than 10 weeks after the end of the active red team testing phase, to the CT, which in turn delivers the BTTR to the RTT and TM. The BTTR should be drafted ahead of the replay and PT exercises. In the BTTR, the BT maps its actions alongside the RTT's actions. Both reports are expected to contain a timeline of events and detections that occurred during the exercise together with any other relevant information. Normal holidays can be taken into consideration when setting deadlines for these reports.

The RTTR and BTTR are highly sensitive. As such, access to these reports, their dissemination, retention and destruction must be controlled. At the request of the TM, the reports might be cleared of sensitive information. This can for instance be machine names, IP addresses, etc.

The TM assesses the RTTR and BTTR contain the required information and provides feedback where necessary. Given the importance of the RTTR for the BTTR and the replay exercise, the TM is advised to provide feedback on the document once in a final stage.

Relevant documents for this process:

- TIBER-EU Red Team Test Report Guidance
- TIBER-EU Blue Team Test Report Guidance

Deliverables:

- Red Team Test Report
- Blue Team Test Report

5.1.1 Create draft Red Team Test Report

The RTTR is a deliverable which should minimum include the information in the TIBER-EU Red Team Test Report Guidance document.

If internal testers are used in the testing, this should be stated in the Red Team Test Report.

When ready, RT should deliver the draft RTTR to the CT, which in turn delivers it to TM, to receive feedback.

Responsible: RTT
Deadline: 4 weeks after active testing is complete
References:
- TIBER-EU 9.2
- TIBER-EU RTTR Guidance
- RTS Art. 12(2) and Annex V

The RT should deliver the draft RTTR to the CT, which in turn delivers it to the BT and TM, within four weeks after the end of the active testing phase.

5.1.2 Review draft Red Team Test Report

The CT and TM review the draft Red Team Test Report and give feedback to RTT based on the TIBER-EU Red Team Test Report Guidance and checks the report documents the red team test and the results sufficiently. The CT should not alter the conclusions if the CT does not agree with these, since the CT can comment on such issues in the Test Summary Report.

Responsible: CT
References:
- TIBER-EU 9.2

5.1.3 Complete final Red Team Test Report

Based on the feedback from both the CT and possibly the TCT, the RTT completes a final version of the RTTR.

The TM will then approve the report in the Approve process which is further described in “Approve final RTTR”.

Responsible: CT
References:
- TIBER-EU 9.2
- TIBER-EU RTTR Guidance
- RTS Art. 12(2) and 12(3)

5.1.4 Create Blue Team Test Report

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 (BTTR). In the BTTR, the BT maps its actions alongside the RTT's actions. The BT can be informed and start creating the BTTR as soon as the RT test execution is finalised. A draft version of the Blue Team Test Report should be ready ahead of the replay exercise to maximise the learnings from the replay.

Responsible: BT
Deadline: 10 weeks after active testing
References:
- TIBER-EU 9.2
- TIBER-EU BTTR Guidance
- RTS Art. 12(4) and Annex VI

The BTTR should at least include the elements detailed in TIBER-EU 9.2 and the TIBER-EU Blue Team Test Report guidance document.

The BT should deliver the BTTR within 10 weeks after the end of the active testing phase to the CT, which in turn delivers it to the RTT and TM.

5.2 Replay process



Within 10 weeks from the active red team testing, CT arranges a replay exercise. Although the exercise should be held within 10 weeks after the end of the active red team testing, it is highly recommended for the exercise to take place after the BTTR has reached a substantial form. The goal of this exercise is to learn from the testing experience in collaboration with the RTT.

During the replay exercise, the RTT and BT jointly go through the actions each of the teams has taken during the test, based on the timeline of events agreed to in the reports. They discuss the conducted attack steps and all related issues of interest to allow the BT to gain a deeper understanding of the technical workings behind the actions taken by the RTT and the established or potential future countermeasures.

The findings and learnings of the replay exercise will feed directly into the final Test Summary Report (TSR) and remediation plan.

Relevant documents for this process:

- TIBER-EU Framework
- TIBER-EU Purple Teaming Guidance
- Red Team Test Report
- Blue Team Test Report

5.2.1 Replay exercise

During the replay exercise, the RTT and the BT go through the tested scenarios step by step to discuss:

- The progression through attack stages of each scenario and relevant learning generated
- What else could have been achieved by the RTT with more time and resources
- Potential remediation measures
- General questions from the BT

Responsible: CT
Participants: RTT, BT, TM, (TIP)
Type: Physical
Typical duration: 4 hours - 2 days
Deadline: 10 weeks after RT
References:

- TIBER-EU 9.2
- RTS Art. 12(5)

The replay exercise must take place within ten weeks after the end of the active testing. This exercise shall be held as a physical meeting.

Preparation:

- RTTR and a draft BTTR

Agenda:

- RTT presentation of attacks
- BT response to attacks
- Discussion on alternative actions taken
- Possible courses for remediation
- Possible actions not sufficiently covered by active testing

Outcomes:

- Better understanding of what happened
- List of possible remediation actions
- Areas for Purple Teaming

The CT should consider involving the TIP in the replay exercise 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.

5.3 Purple Teaming process



After the completion of the replay exercise, a PT exercise should be conducted, in which the RTT and the BT come together to discuss all remaining or additional topics relevant to the CT and the BT. This exercise is highly beneficial for increasing the learning experience of the entity, anchoring the learnings of the test within the organisation. Potential topics for the PT exercise should be jointly identified by the CT, RTT and the BT and could range from a table-top discussion to technical walkthroughs of the systems.

During the PT exercise, the BT and the RTT further elaborate on the scenarios that have been played out. This exercise allows the stakeholders to discover alternative scenarios and their potential consequences, maximising the learning effect of the overall test.

Although the exercise should be held no later than 10 weeks after the end of the active red team testing, it is highly recommended for the exercise to take place after the BTTR has reached a substantial form.

Relevant documents for this process:

- Red Team Test Report
- Blue Team Test Report
- TIBER-EU Purple Teaming Guidance

Deliverables:

- Purple Teaming Exercise is executed

5.3.1 Purple teaming exercise

Responsible: CT
Participants: RTT, BT (TIP)
Typical duration: Varies
Deadline: 10 Weeks after RT
References:

- TIBER-EU 9.4
- TIBER-EU Purple Teaming Guidance
- RTS Art. 11(5) and 12(5)

In the purple teaming exercise, the BT and the RTT work closely together to see which other steps (in systems or processes) could have been taken by the RTT, and how the BT could have responded to those steps.

Purple teaming can also cover table-top exercises based on the 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.

The PT exercise must take place within ten weeks after the end of the active testing, and a replay exercise must be conducted beforehand.

Preparation

- Prepare purple teaming activities with the CT and the BT. Responsible: RTT.

Agenda

- Relevant issues not tested during active testing
- Vulnerabilities identified during the test
- Other steps not taken by RTT and potential BT responses
- Alternative scenarios and potential consequences
- Proof of concept
- Discussion of anticipated remediation measures with the RTT
- Business continuity exercises

Outcomes:

- Training of the BT capabilities and processes

5.3.2 Restoration

Responsible: RTT (TIP)
Participants: CT, BT
References:
- TIBER-EU 8.4
- RTS Art. 7(1)(g) and (h)

After all testing activities are completed, the RTT and possibly TIP should carry out restoration procedures to safeguard the integrity of the tested entity's environment. These restoration procedures should be planned and coordinated with the CT and BT, and ideally not occur before the replay and PT exercise in the closure phase. The RTS Art. 7(1)(g) "at the end of testing" should be interpreted in this way, not the end of the testing phase and before the closure phase .

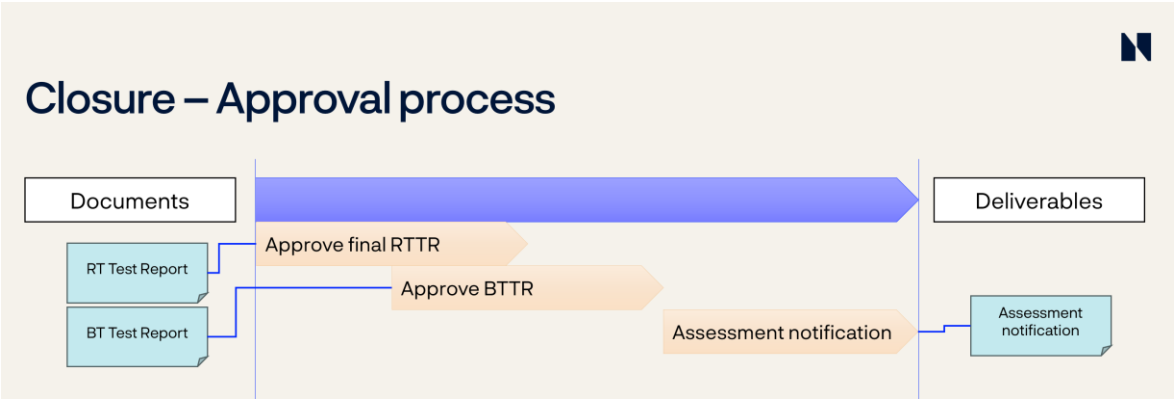
The procedures include the deletion of information related to passwords, credentials (or changing them) and other (secret) keys compromised during the test. It also includes the restoration and deletion of compromised secure communication channels to the entity, secure collection, storage, management and disposal of collected data.

Technical restoration procedures should include:

- Command and control deactivation
- Scope and date kill switches
- Removal of backdoors and other malware
- Potential breach notification
- Procedures for future back-up restoration which may contain malware or tools installed during the test

Monitoring of the BT activities and information to the CT of any possible detections

5.4 Approval process



The TM assesses the RTTR and BTTR contain the required information and provides feedback where necessary. Given the importance of the RTTR for the BTTR and the replay exercise, the TM is advised to provide feedback on the documents once in the final stage.

Relevant documents for this process:

- Red Team Test Report
- Blue Team Test Report
- TIBER-EU Blue Team Test Report Guidance
- TIBER-EU Red Team Test Report Guidance

Deliverables:

- Feedback from TCT and TM

5.4.1 Approve final RTTR

To verify the test has been conducted in line with the TIBER framework, the TM will review the final Red Team Test Report.

Responsible: TCT
References: TIBER-EU 9.2

The TM shall verify the contents towards the TIBER-NO Approval Checklists for RTTR. After the RTTR is successfully approved, the TM should notify the CTL of its validation by written feedback.

5.4.2 Approve BTTR

The TM shall verify the contents towards the TIBER-NO Approval Checklists for BTTR. After the BTTR is successfully approved, the TM should notify the CTL of its validation by written feedback.

Responsible: TCT
References: TIBER-EU 9.2

5.4.3 Create assessment notification

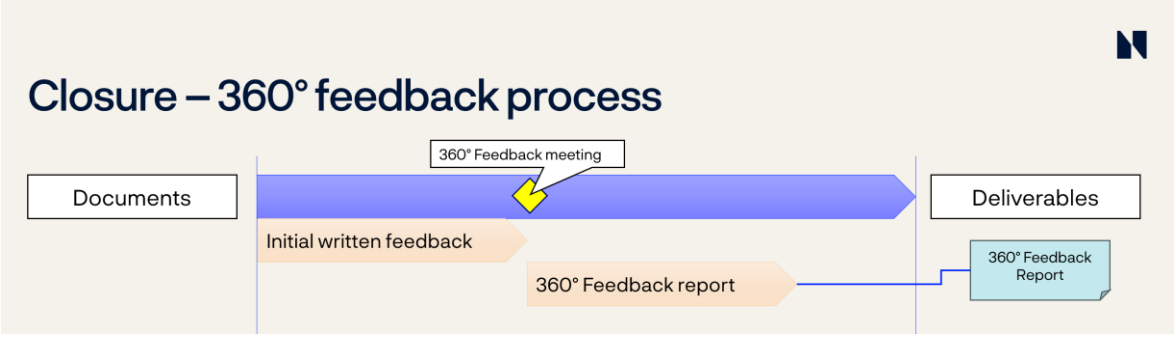
After the TCT has evaluated the RTTR and the BTTR, an assessment notification shall be created and shared with the CT.

The date of the notification marks the start of the remaining time allocated to the closure phase before the final attestation takes place.

Responsible: TCT
References:

- TIBER-EU 9.2
- RTS Art. 12(7)

5.5 360° Feedback process



The goal of the 360° feedback process 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 360° Feedback Report is used to collect feedback.

The dedicated 360° feedback meeting, organised by the TM, is focused on providing feedback to all the stakeholders involved in the testing process. This meeting allows for the participants in the test to reflect upon and improve their approach for future tests. In addition, it also creates the possibility to provide feedback on the testing process as well as the TIBER-EU and TIBER-NO framework.

Relevant documents for this process:

- TIBER-NO 360° Feedback Report

Deliverables:

- 360° Feedback Report

5.5.1 Initial written feedback

The TM sends out a template for feedback, the TIBER-NO 360° Feedback Report. Each of the CT, TIP, RTT and BT fill inn answers to the questions in the template and return this to the TM. The TM will also answer the questions.

Responsible: TCT
Deadline: 2 weeks before 360° meeting
References:

- TIBER-EU 9.7
- RTS Art 12(6)

This should be completed two weeks before the 360° feedback meeting. Before this meeting, the TM will send out a draft version with the collected feedback from each party to the participants one week in advance of the 360° feedback meeting.

5.5.2 360° feedback meeting

A 360˚ feedback meeting is held between all stakeholders to review the TIBER test. All parties should deliver feedback on each other and on the overall process to facilitate the learning experience for future exercises. 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 draft 360° Feedback Report.

Responsible: TCT
Participants: CT, TIP, RTT, BT
Type: Physical
Typical duration: 2 hours
References:

- TIBER-EU 9.7
- RTS Art 12(6)

Preparation

- Draft TIBER-NO 360° Feedback Report

Agenda

- Walk-through of the aggregated input and further comments by each party
- Suggested updates to TIBER-NO
- Any other feedback

Outcomes:

- Basis for 360º Feedback Report
- Possible updates to TIBER-NO

The 360° feedback meeting should take place before the TM approval of the Test Summary Report and the Remediation Plan.

5.5.3 360° Feedback Report

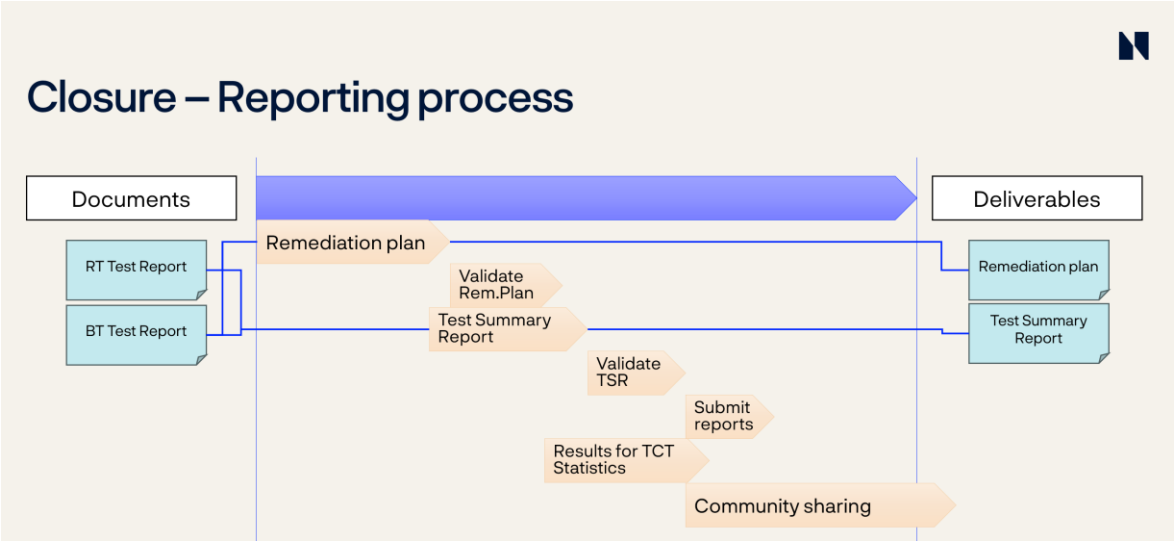
The TCT collects further feedback given in the 360° Feedback Meeting and incorporates into the previously distributed draft 360° Feedback Report. The final version is then distributed to the participants.

Responsible: TCT
References:

- TIBER-EU 9.7
- RTS Art 12(6)

The TM may share the output from the 360° Feedback Report on an anonymous basis with the TIBER Knowledge Centre, so all lessons learned 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 in the TIBER framework.

5.6 Reporting process



Relevant documents for this process:

- Scope Specification Document
- Targeted Threat Intelligence Report
- Red Team Test Plan
- Red Team Test Report
- Blue Team Test Report
- TIBER-EU Test Summary Report Guidance
- TIBER-EU Remediation Plan Guidance

Deliverables:

- Remediation Plan
- Test Summary Report

5.6.1 Remediation Plan

The remediation plan is, in addition to the replay and PT exercises, also based on the TTIR, BTTR and RTTR. Its aim is to plan improvements, and the mitigation of vulnerabilities and their root causes identified during the test.

The remediation plan should cover the elements described in TIBER-EU 9.6 and the TIBER-EU Remediation Plan Guidance.

Responsible: CT
Deadline: 8 weeks after assessment notification
References:
- TIBER-EU 9.6
- RTS Art. 13(1) and 13(2)

The remediation plan should be delivered to the TM, within eight weeks after the TM has sent a notification of the completed assessment of the RTTR and BTTR. If requested by the TM, a version not containing any sensitive information should be provided instead.

5.6.2 Validate Remediation Plan

The TM validates the content of the remediation plan towards the requirements specified in the TIBER-NO Approval Checklists. After the remediation plan is successfully validated and complete, the TM should notify the CTL of its approval by written feedback.

Responsible: TCT
References:
- TIBER-EU 9.6 and 9.8
- RTS Art. 13(1) and 13(2)

5.6.3 Test Summary Report

The Test Summary Report (TSR) highlights the overall test process and results, and should draw on the test documentation, such as the RTTR, the BTTR, the TTIR as well as the RTTP. If the test were using internal RTT, this should be stated in the TSR.

The TSR must include at least the elements detailed in TIBER-EU 9.5 and the TIBER-EU Test Summary Report Guidance.

The TSR should be delivered by the entity to the TM, within eight weeks after the TM has sent a

Responsible: CT
Deadline: 8 weeks after assessment notification
References:
- TIBER-EU 9.5
- TIBER-EU Test Summary Report Guidance
- DORA Art. 26(6)
- RTS Art. 12(7), 15(3) point (c) and Annex VII

notification of the completed assessment of the RTTR and BTTR. The TM shall approve the TSR. If requested by the TM, a version not containing any sensitive information should be provided instead.

5.6.4 Validate Test Summary Report

The TM validates the content of the TSR toward the TIBER-NO Approval Checklists for TSR. After the TSR is successfully validated and complete, the TM should notify the CTL of its approval by written feedback.

Responsible: TCT
References:
- TIBER-EU 9.8 and 9.5

5.6.5 Submit reports to Competent Authority (DORA TLPT)

If the TIBER test is part of a DORA TLPT test, the Remediation Plan and the Test Summary Report shall be submitted to the Competent Authority, being Finanstilsynet in Norway. When ready, also the attestation shall be submitted.

Responsible: CT
Deadline: 8 weeks after assessment notification
References:
- TIBER-EU 9.5
- DORA Art. 26(6)
- RTS Art. 12(7)

The Competent Authority might follow up on the results of the TIBER engagement after the test is completed, including the Remediation Plan. However, a TIBER test is a learning experience for self-improvement and TIBER tests are snapshots rather than comprehensive assessments. The follow-up of results should therefore be conducted in the appropriate spirit.

5.6.6 Results for TCT Statistics

The TCT will not share any information or documentation from the test with any outside party. However, as one of the key objectives of the TIBER-NO and TIBER-EU is to enhance sector resilience and contribute to financial stability, TCT collects some information from each TIBER test. TCT further analyzes this information to aggregate results which later will be shared with relevant stakeholders.

Responsible: TCT
References: TIBER-EU 9.8

The information needed will be requested from both CT and RTT during the closure phase from the TM.

All information which is collected will be anonymized in the aggregated results and no information will be connected to the tested entity. The information collected will give insight into common threats and vulnerabilities, key findings as well as information related to the execution of the test. The goal with these results is to form a picture of the resilience of the Norwegian financial sector as well as lessons learned and suggestions for improvements of the TIBER-NO framework.

The results may also be shared with TIBER Knowledge Center (TKC) which is a group of European TCTs.

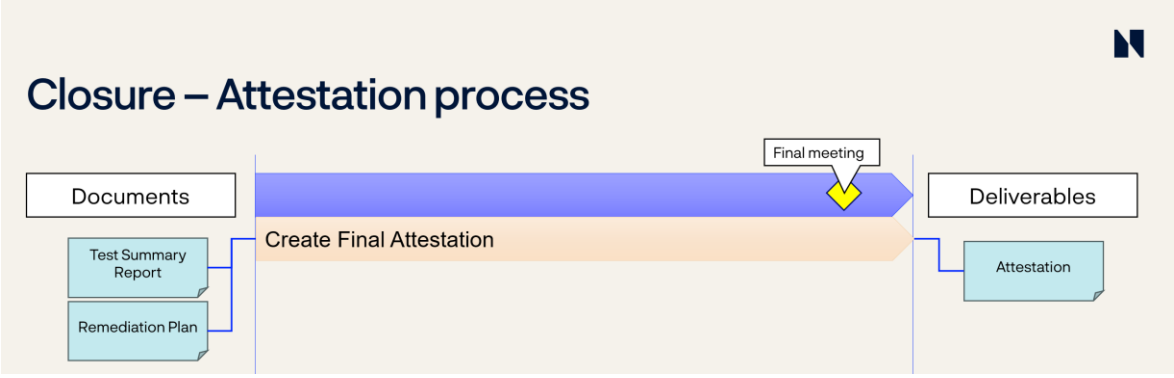
5.6.7 Community sharing in TIBER-NO Forum

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.

Responsible: CT
References: TIBER-EU 9.8

The completion of this activity may occur also after the test has been completed.

5.7 Attestation process



At the end of the test, once the TIBER authority has approved the TSR as well as the remediation plan, the TIBER authority should provide an attestation confirming the test was conducted in accordance with the core requirements of the TIBER-EU framework. The attestation should be signed by the TIBER authority. The issuing of the attestation concludes the TIBER test.

A TIBER test attestation can serve as a means of qualifying the test for mutual recognition among other authorities. In cases where other TCTs did not participate in the test but there was mutual agreement to share the test results, the entity should share the TSR, the remediation plan and the attestation. The TSR serves as a form of assurance the test has indeed been conducted, and the attestation qualifies the test as a legitimate TIBER test.

Relevant documents for this process:

- TIBER-EU Attestation Guidance
- Test Summary Report
- Remediation Plan
- 360° Feedback Report

Deliverables:

- Final Attestation

5.7.1 Create Final Attestation

After the TM has approved the TSR and remediation plan, a final attestation shall be created. In addition, all mandatory requirements in the TIBER-NO Approval Checklists shall be met.

Responsible: TCT
References:
- TIBER-EU 9.8
- DORA Art. 26(6) and 26(7)
- RTS Art. 14(1), 14(2) and Annex VIII

The attestation document should include at least the elements described in TIBER-EU 9.8 and the TIBER-EU Attestation Guidance.

The attestation shall be presented to the CTL.

If other authorities have been involved in the test, the attestation shall be distributed to these authorities as well.

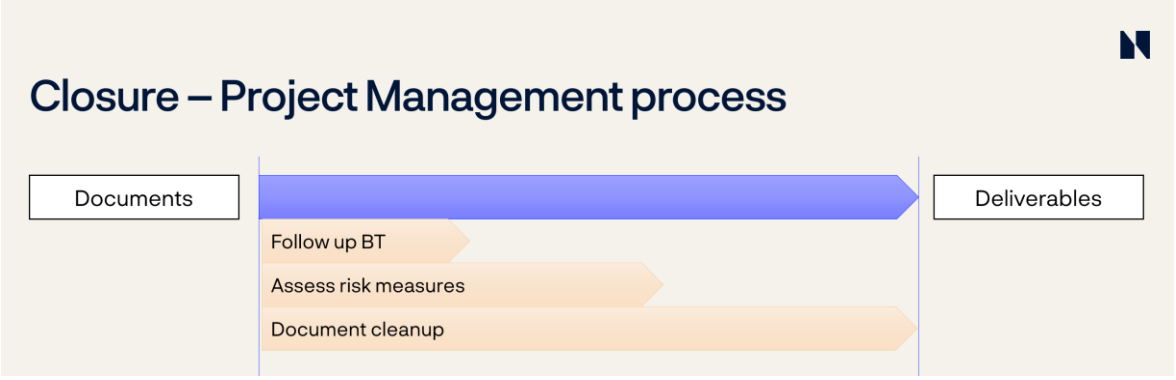
5.7.2 Final meeting

At the end of the test process, a final meeting between the TCT and the CT 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.

Responsible: TCT
Participants: CT
Type: Physical or online
Typical duration: 1 hour
References: None

Agenda
- Formal closure of test
- Any outstanding action points
- Sharing of learnings
- Next TIBER-NO test

5.8 Project management process



After the testing has concluded, the test shall be wrapped up adequately. Also, learning should be stored for upcoming tests.

5.8.1 Follow up blue team

Responsible: CT
References: RTS Art. 12(1)

When the active testing is finished, the CTL should inform the Blue Team a TIBER took place.

The CTL and CT should also make sure to follow up the BT during the closure phase. They should make sure appropriate time is set aside for them to do their tasks (write BTTR, attend PT and other exercises/meetings). In addition, the CT should also follow up the workload on the BT in this period. There may be a lot of (unexpected) work over a short period of time.

5.8.2 Assess risk measures

Responsible: CT
References: TIBER-EU 7.2.2

Even though the active testing is completed at this stage, the CT should assess their risk management controls also in this phase. The test has most likely identified vulnerabilities and areas for improvement which constitutes a risk for the entity also after the TIBER test is completed.

5.8.3 Document cleanup

Responsible: CT
References: None

Any outstanding points in the action log will be closed and an agreement on when to close the common document folders will be made. If shared channels like Teams are created, it is decided when they should be closed. Important documents need to be stored elsewhere if needed for future tests or for documentation of the conducted test.

Also, how to share the learnings, which can be used by other organisations to enhance cyber resilience, may be discussed.

Appendix A: Abbreviations

BT: Blue Team

BTTR: Blue Team Test Report

CIF: Critical or Important Function

CT: Control Team

CTL: Control Team Lead

DORA: Digital Operational Resilience Act

GTL: Generic Threat Landscape

ICT: Information and Communication Technology

OSINT: Open-Source Intelligence

PT: Purple Teaming

RTS: Regulatory Technical Standard

RTT: Red Team Testers

RTTP: Red Team Test Plan

RTTR: Red Team Test Report

TCT: TIBER Cyber Team

TIBER: Threat Intelligence-Based Ethical Red Teaming

TI: Threat Intelligence

TIP: Threat Intelligence Provider

TKC: TIBER-EU Knowledge Centre

TLPT: Threat Led Penetration Testing

TM: Test Manager

TSR: Test Summary Report

TTIR: Targeted Threat Intelligence Report

TTP: Tactics, Techniques and Procedures

Appendix B: Change log

Version	Date	Change
2.3.1	26.10.2026	Swapped section 2.3.5 Approve scope and 2.3.6 Validate scope and added that Finanstilsynet comments on scope. Removed broken bookmark links. (AH)
2.3	25.09.2026	Removed section 1.2 with document list, as this is now maintained on web pages. Removed references to retired TIBER-NO Scope Specification Template. Added some phasis on business overview in section 3.1. Removed reference to Finanstilsynet's discontinued e-mail address in 2.3.3. Smaller editorial updates. (AH)
2.2	10.04.2026	Added flag descriptions in sections 2.3 Scoping, 3.2 Scenario Creation, 3.3 TTI Report creation and 4.1 RT test plan creation. Added RTTP may deviate from TTIR in section 4.1.1. Added new section 4.3.6 Information to Blue Team. Switched order of reporting and 360° processes in closure phase. Added reference to TIBER-EU in 5.6.3 Test Summary Report (AH)
2.1	04.11.2025	Added naming convention to section 2.3 Scoping, moved section 3.4.1 Validate Providers to correct location at section 2.4.5, new section 4.3.3 Submit leg-ups and miscellaneous smaller clarifications and editorial updates. (AH)
2.0	12.08.2025	Major update for new version of TIBER-EU and DORA TLPT. (AH)
1.3	11.06.2024	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. (AH)
1.2.1	25.10.2023	Added sentence on internal RT in section 3.2. Updated external document references. (AH)
1.2	05.10.2023	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. (AH)
1.1	21.03.203	Language reverted back to English. Added RACI matrix as Appendix A. Minor editorial and formatting updates. (AH)
1.0	01.01.2023	Initial version translated to Norwegian based on document from TCT-DK. (AH)