# TIBER-NO
# Red Team Test Plan Guidance

Version 0.1

## 1 Introduction

This is practical guidance produced by TCT-NO to support and guide how to produce the Red Team Test Plan (RTTP) in TIBER-NO tests. The figure below shows the Red Team test phase in the TIBER-EU process.

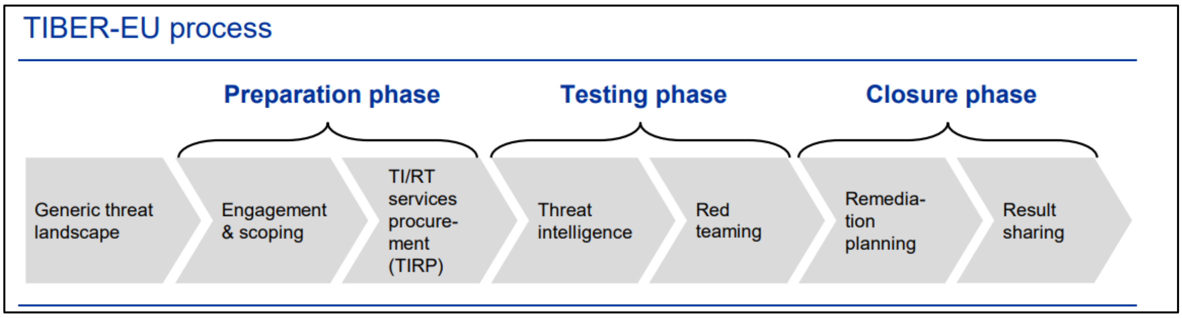


*Fig: TIBER-EU process*

### 1.1 How to use this document

This documented is intended as a supporting document to the official guidance from TIBER-EU (1), specifically catered to Norwegian TIBER tests. It is primarily intended for the Red Team provider to understand the process and providing the best possible deliverable to TIBER tests.

This guide is based on:

- TIBER-EU Guidance for the Red Team Test Plan document.
- TIBER-NO Operational Guide v1.2, “3. Red Team test phase”

For more general information about TIBER-EU and TIBER-NO, see:

- What is TIBER-EU? and the TIBER-EU Framework
- TIBER-NO and TIBER-NO implementation Guide

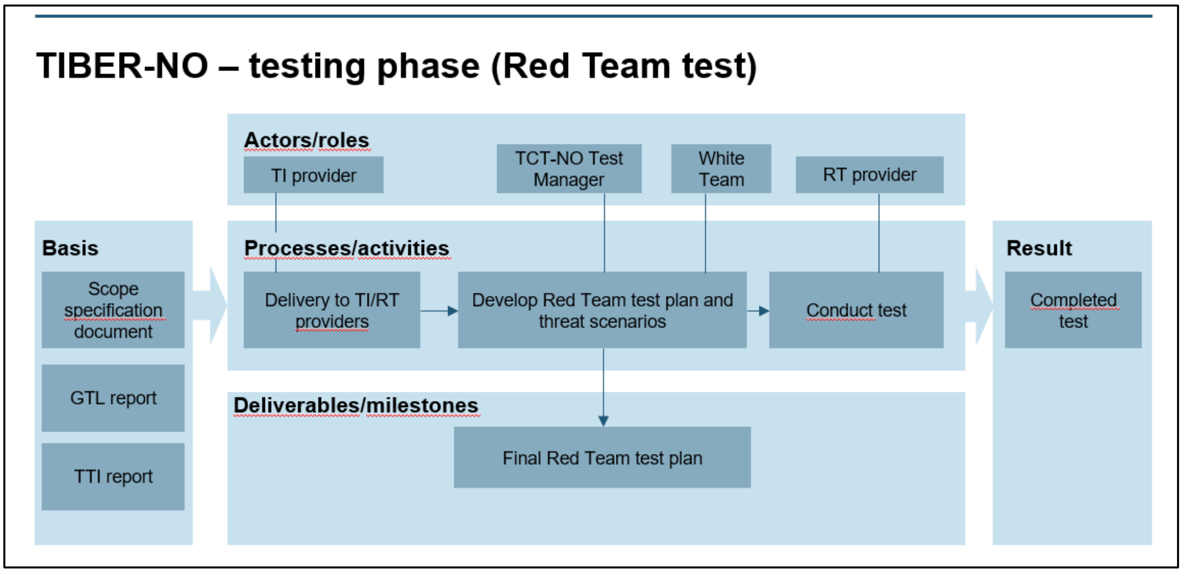
### 1.2 The Red Team Test phase in TIBER-NO

The Red Team Test phase does not differ in any way from the way it is described in the European TIBER-EU framework. This means the official RTTP guidance from TIBER-EU Framework can be used to support TIBER-NO tests. This guide is merely meant to clarify and supplement that guide. Detailed requirements are outlined in the main Framework document. The guidance is not mandatory and may be deviated from.

## 1.3 About the Red Team Test Plan

The RTTP is a document to support the TIBER test and provide the White Team with an overview of the active testing phase of the TIBER test. The RTTP is shared with the WT and the TCT(s) for the jurisdiction the test takes place in. The WT and TCT need to agree and attest on the RTTP contents before the test can progress.

The RTTP is also shared with the TI team. This allows them to help the RT ensure the plan aligns with the scenarios proposed in the Targeted Threat Intelligence Report, the Entity, the importance of the Critical Functions and relevant threats to both. The report enables them to assist the RT with developing the RT Test Plan and later in the attack phase, to maintain the realism for the test, and rationalize attack techniques and operational security choices during testing.



TIBER-NO – testing phase (Red Team test)

Actors/roles

TI provider

TCT-NO Test Manager

White Team

RT provider

Basis

Scope specification document

GTL report

TTI report

Processes/activities

Delivery to TI/RT providers

Develop Red Team test plan and threat scenarios

Conduct test

Result

Completed test

Deliverables/milestones

Final Red Team test plan

*Fig: TIBER-NO RTT process*

## 1.4 Input to the Red Team Test plan

The Red Team test plan requires input from a range of different sources. The RT provider should use information from the scope specification, the TTI report, and risk management workshops to form a plan for the test that matches the scope, threat intelligence and goals of the test. The inputs are:

- Scope Specification document produced by the WT.
    - Should include Critical Functions, underlying key systems and services, flags, targets, and objectives of the test. This allows the RT provider to increase its knowledge of the entity and to focus its test plan on targeting the Entity and its critical function.
- Targeted Threat Intelligence report

    - Especially the threat actors and high-level scenarios, as well as any useful information from the digital footprint operation the TI team has performed.
- Risk assessment performed with the WT
    - As the Red Team needs to address operational risk in the test, the risk assessments performed with the WT should be used as valuable input when describing risk in each test scenario.

# 2 Contents of the Red Team Test plan

This section describes the contents and development of the RTTP.

## 2.1 Introduction to the plan and test

- Code name: Describe the code name for the test and how this is used to maintain the secrecy of the test, both during planning and execution of the test.
- Project plan: Describe a timeline for the threat scenarios, ensure adequate time is scheduled for each scenario and that any potential delays ar.

## 2.2 Organization of the test

- Team composition
    - Roles and responsibilities: Describe the roles and responsibilities for the Red Team, especially lead, manager and/or contact points for the White Team.
    - Team members: Describe the competence of Team Members and how they match the scope for test. Note any changes to the team based on new information.
- Communication channels
    - Describe how the RT will communicate with the other involved parties, especially the WT
    - Describe the Escalation chain for events that may require escalation
- Risk management
    - Describe the risk management and controls of the Red Team. Address:
        - Rules of Engagement and ethics
        - Out of bounds / out of scope components
        - Logging and auditing during the test
- Leg-up process
    - Describe the leg-up process for handling leg-ups, both pre-planned and future, as this often involves careful coordination and collaboration among various teams and stakeholders. Provide here is a description of how leg-ups should be planned, approved, executed and reported to maintain the realism of the test and not add doubt to the test results.

## 2.3 Scenario descriptions

The RTTP should describe each individual scenario. They do not have to align perfectly with the scenarios proposed in the Targeted Threat Intelligence report, but any deviances should be aligned with and supported by the TI provider and the WT.

Each scenario should describe:

- Attacker motive, intent, and operational strategy
    - The main objective of the threat actor in this scenario, their approach and how they use the access they gain through the attack to achieve their goals. Additionally, their agility, for example if they are willing to change from “low-and-slow” to a “smash-and-grab” operation in the event of failure or detection.
- Critical Functions (relevance) – supported by Threat Intelligence
    - Describe the relevance here for the specific scenario critical functions and high-level objectives which are based on the scoped objectives provided by Entity in combination with the threat intelligence as outlined in the Targeted Threat Intelligence report.
- Attack flow
    - Describe the flow of the proposed attack scenario. detailing steps for the IN, THROUGH and OUT phases.
    - Each scenario should include a visual diagram of the proposed attack paths, ideally with leg-ups, flags and key sections of the attack clearly indicated.
    - The primary TTPs (Mitre ATT&CK) to be used by the Red Team to emulate the threat actor. This should align with the TTI report but can deviate given the selected techniques are still within the range of realism for the given threat actor.
- Leg-ups
    - Describe how leg-ups will be applied with clear justification and requirements. It can be beneficial to set a concrete deadline for timesaving leg-ups. See the TIBER-NO leg-up guidance for how to describe leg-ups in detail. The leg-ups can be drawn into the attack path or visual diagrams if possible.
- Risk management controls
    - Describe any additional risk factors or implemented controls for operational risk in the Red Team test. Note down any risks identified specifically for the described test scenario. E.g., some threat actors perform risky actions like exfiltrating data over unencrypted protocols, which may be a risk the RT and WT cannot accept.

# 3 Example RTTP structure

*This is just an example of some components of what a RTTP should include, not an exhaustive list. TIBER-NO does not provide a template for the plan itself.*

- Introduction
    - Organization of the test
    - Project planning
    - Team composition
    - Communication protocols
    - Risk management
    - Leg-up process
- Attack scenarios
    - Details for each attack scenario
- Appendices
    - For larger amounts of information, TTP tables, or similar.

# 4 TIBER-EU recommendations for RTTP

These are not strict *requirements*, but recommendations from the TIBER-EU guidance for the RTTP.

- The TI provider holds a handover session with the RT provider, providing the basis for the threat scenarios.
- The TI provider continues to be engaged during the testing phase and provides additional up-to-date, credible threat intelligence to the RT provider, where needed.
- The RT provider develops multiple attack scenarios, based on the TTI Report. This is documented in the Red Team Test Plan and shared with the WT and TCT.
- The RT provider executes the attack based on the scenarios (with some flexibility) in the Red Team Test Plan and goes through each of the phases of the kill chain methodology.
- During the test, the RT provider keeps the WT and TCT informed about progress, “capture the flag” moments, the possible need for leg-ups, etc.
- The RT provider takes a stage-by-stage approach and consults the WT and TCT at all critical points to ensure a controlled test.
- The duration of the red team test is proportionate to the scope, size of the entity, complexity of threat scenarios, etc.

### Checklist for the RTTP from TIBER-EU

These are recommendations extracted from the TIBER-EU guidance for the RTTP. This can serve as a checklist for the RT provider when developing the plan to ensure they include the minimum information required. TCT-NO encourages the RT provider to use this table in that manner.

| Category | Element | Desc. |
|---|---|---|
| Organisation | Team composition | The RT provider should select a team that has the competencies that match the scope |
| Organisation | Code name | Throughout the Red Team Test Plan, the RT provider should use the code name assigned to the entity instead of the real name of the entity. |
| Organisation | Communication channels | The RT provider should indicate how they are planning to keep the stakeholders (i.e. White Team, TCT and TI provider) updated during the testing process. All communication must be conducted via secured channels, for example, end-to-end encrypted chat and email. During active communications in the test, the participants should refer to the entity by its codename instead of the real name to minimize risk in case of communication leaks |
| Organisation | Risk management | The risk management approach should set out how the RT provider will take the appropriate actions before, during and after the test. |
| Organisation | Leg-up process | Leg-up design and activation is specified in the TIBER-NO Leg-ups Design Document.<br>Leg-ups follow test scenarios. The same leg-up can be used for multiple scenarios, but has to be uniquely defined.<br>Leg-ups have a code and a description, which includes a reason for the use of the leg-up, the leg-up type, what is its compensating for and what the requirement for activation is. |
| Project planning | Timeline | The RT provider should provide a general timeline that is used for the execution of the scenarios |
| Attack scenarios | Critical functions | The relevance of the critical function being tested, and how the flag/objective relates to the critical function and its underlying systems and services. |
| Attack scenarios | Attacker motive and intent | Based on the collected threat intelligence in the TTI Report, elaborate in further detail and more precisely what the motives and intent of the threat actors are;<br>how they would seek to target the specified critical functions<br>which of the CIA triad they would seek to compromise<br>and how they would focus their efforts on achieving the final flags. |
| Attack scenarios | TTPs | What tactics, techniques and procedures the threat actor would use to achieve the specific flags. These TTPs should be set out in line with the MITRE ATT&CK Framework. |

| Category | Element | Desc. |
|---|---|---|
| Attack scenarios | Leg-ups | The potential leg-ups that will be required in case the RT provider is unable to achieve the flag/objective within its specified timeline (as prescribed in the project plan). For each leg-up, the RT provider should clearly state what it entails, who is responsible for granting it, and what process and protocol must be invoked to use the 2 https://attack.mitre.org/ TIBER-EU: Guidance for the Red Team Test Plan 10 leg-up. It should also illustrate any relationship between the different scenarios and show dependencies on leg-ups in order to visualize the orchestration of the test. |
| Attack scenarios | Risk management controls | The risk management controls that the RT provider will have in place to manage any risk stemming from implementing the attack scenario. Due to the inherent risk in conducting a TIBER test, it is essential that the RT provider applies appropriate controls for each attack scenario, and communicates these to the White Team. |

## Change log

| Version | Date | Change |
|---|---|---|
| **0.1** | 17.10.2023 | Initial version |