Norges Bank

TIBER-NO

Red Team Test Plan Guidance

Version 2.2

TLP:CLEAR

This is practical guidance to support and guide how to produce the Red Team Test Plan (RTTP) in TIBER-NO tests. It is primarily intended for the Red Team Testers to understand the process and enable them to provide the best possible deliverables to TIBER tests.

04.02.2026

Contents

1	**Introduction**	**2**
1.1	The Red-Teaming test phase in TIBER-NO	2
1.2	About the Red-Teaming Test Plan	2
1.3	Input to the Red Team Test Plan	3
2	**Contents of the Red Team Test plan**	**4**
2.1	Introduction to the plan and test	4
2.2	Organization of the test	4
2.3	Scenario descriptions	4
3	**Example RTTP structure**	**5**

1 Introduction

This documented is intended as a supporting document to the official guidance from TIBER-EU, specifically catered to Norwegian TIBER tests.

This guide is based on:

- TIBER-EU Red Team Test Plan Guidance document
- TIBER-NO Operational Guide, “4. Testing phase: Red-Teaming”

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

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

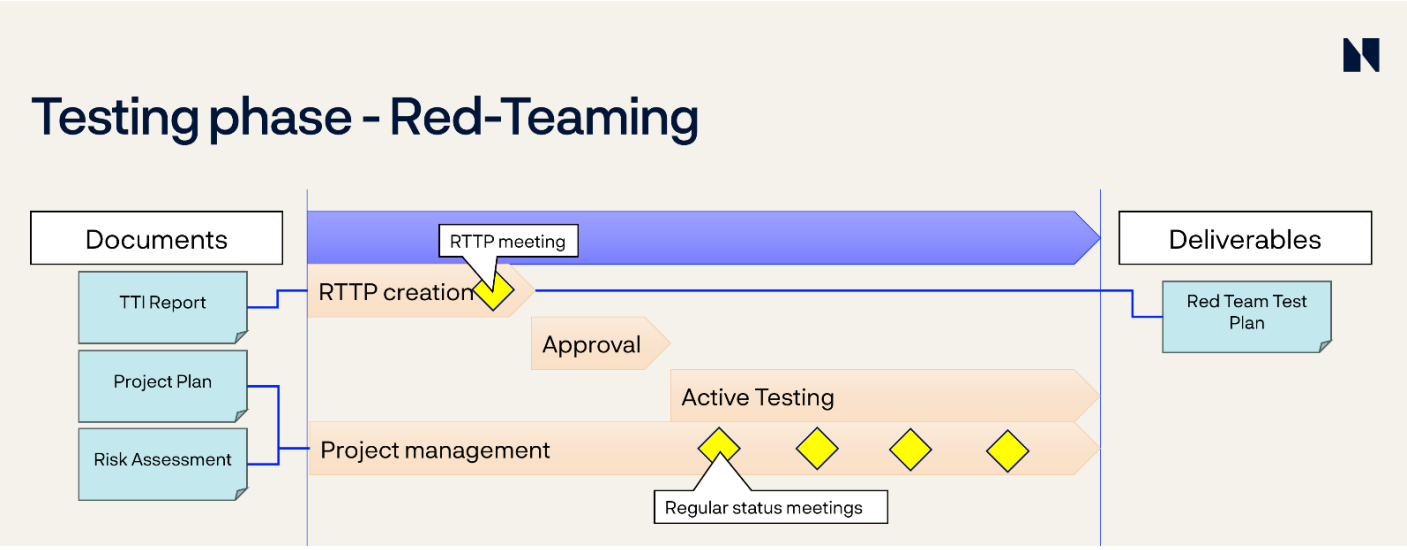
1.1 The Red-Teaming test phase in TIBER-NO

The Red-Teaming 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.

1.2 About the Red-Teaming Test Plan

The RTTP is a document to support the TIBER test and provide the Control Team with an overview of the active testing phase of the TIBER test. The RTTP is shared with the CT and the TCT(s) for the jurisdiction the test takes place in. The CT 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 RTT ensure the plan aligns with the scenarios proposed in the Targeted Threat Intelligence Report, the Entity, the importance of the Critical and Important Functions and relevant threats to both. The report enables them to assist the RTT with developing the RTTP and later in the attack phase, to maintain the realism for the test, and rationalize attack techniques and operational security choices during testing.



1.3 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 CT.
    - Should include Critical and Important Functions, underlying key systems and services, flags, targets, and objectives of the test. This allows the RTT to increase its knowledge of the entity and to focus its test plan on targeting the Entity and its critical and important 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.
    - The Red Team Test Plan may deviate from the TTIR and the proposed TTPs described, as long as the intensions and motivations of the TA are intact. Such deviations should be described, including reasoning for the change.
- Risk assessment performed with the CT
    - As the Red Team needs to address operational risk in the test, the risk assessments performed with the CT should be used as valuable input when describing risk in each test scenario.

The plan shall be based on the Unified Kill Chain approach with attack flows focusing on IN, THROUGH and OUT phases. Often an unproportionate amount of focus is given to penetrating the perimeter security which is of a relatively high quality, while lesser time and resources are devoted to lateral movement and actions on objectives. Also, the General Threat Landscape Report is based on the Unified Kill Chain approach to threat intelligence.

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 Control 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 RTT will communicate with the other involved parties, especially the CT
    - 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 TIP and the CT.

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 and Important Functions (relevance) – supported by Threat Intelligence
    - Describe the relevance here for the specific critical functions and high-level objectives for the scenario. These functions and objectives 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 Testers to emulate the threat actor. This should align with the TTIR 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 RTT and CT 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.

Changelog

Version	Date	Change
2.2	04.02.2026	Updated illustrations, added info about Unified Kill Chain and deviation in 1.4, Updated visual layout of document (AH)
2.1	23.01.2026	Removed outdated checklist (AH)
2.0	09.04.2025	Updated with new TIBER terminology (AH)
1.0	09.04.2024	Ready for publication (AH)
0.1	17.10.2023	Initial version