24 October 2022

TIBER-NO

Implementation guide

Version 1.0.1

Table of contents

1 Introduction

1.1 Background

Society depends on the functions performed by the payment system and other parts of the financial infrastructure. They enable private individuals and firms to pay for goods and services, and banks to provide financing, while redistributing risk. A secure and efficient financial infrastructure is therefore essential for financial stability. The risk of cyber attacks on this infrastructure is a growing challenge to the efficiency and security of the payment system globally and in Norway.

In 2018, the European Central Bank (ECB) developed a framework for Threat Intelligence-based Ethical Red Teaming (TIBER-EU). The purpose of TIBER-EU is to enable authorities to work with entities under their responsibility to put in place a programme for testing and improving their resilience. It facilitates sharing experience from testing to enhance the cyber resilience of the European financial sector[1]. TIBER-EU has been introduced in a number of European countries, including Denmark, Sweden and Finland.

TIBER-NO implementation guide has been developed jointly by Finanstilsynet (Financial Supervisory Authority of Norway) and Norges Bank, in dialogue with other relevant authorities and the industry.

1.2 What is TIBER-EU?

The TIBER-EU is a European framework developed by the ECB which delivers a controlled, bespoke, threat intelligence-led red team testing of entities' critical live production systems. It helps an entity to assess its protection, detection and response capabilities against sophisticated cyber attacks. The use of capable and experienced third-party providers for Threat Intelligence and Red teaming (testing specialists) ensures that testing is realistic and minimises the possibility of adverse effects. An intelligence-led red team test involves the use of a variety of techniques to simulate an attack on an entity’s critical functions and underlying systems mimicking the tactics, techniques and procedures of real-life threat actors. Conducting this type of tests, helps entities to identify and understand vulnerabilities so that risk reduction measures can be implemented. The objective is for key financial sector participants to be better equipped to uncover, protect themselves against and fend off serious cyber attacks.

TIBER-EU has the following core objectives:

- Enhancing the cyber resilience of entities, and of the financial sector in general.
- Standardising and harmonising the way entities in the EU perform intelligence-led red team tests, while also allowing each jurisdiction a degree of flexibility to adapt the framework according to its specificities.

[1] The framework is based on similar testing programmes in the UK and the Netherlands. See https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html

- Providing guidance to authorities on how they might establish, implement and manage this form of testing at a national or European level.

- Supporting cross-border, cross-jurisdictional intelligence-led red team testing for multinational entities.

- Enabling supervisory and/or oversight equivalence discussions where authorities seek to rely on each other’s assessments carried out using TIBER-EU, thereby reducing the regulatory burden on financial sector entities and fostering mutual recognition of tests across the EU.

- Creating the protocol for cross-authority/cross-border collaboration, result sharing and analysis.

A standardised testing programme ensures comparable security assessments across systems and countries and facilitates information sharing between authorities and entities at a national and international level.

A TIBER test simulates a potential attack by relevant threat actors to test whether the measures implemented by entities are sufficient. The test supplements entities’ periodic security audits, penetration tests and vulnerability scans and can provide a more realistic picture of resilience to cyber attacks.

Under TIBER-EU, the entities tested are responsible for the test. This means that the entity contracts with threat intelligence and red team providers, manages risk, conducts testing and takes responsibility for the summary report and remediation plan. A dedicated team in the entity’s organisation (White Team) is responsible for this.

1.3 About TIBER-NO

TIBER-NO is the Norwegian implementation of TIBER-EU and applies to the financial sector in Norway. The implementation guide (this document) details the Norwegian TIBER implementation within the framework established by TIBER-EU and clarifies the choices made for TIBER-NO.

In its draft Digital Operational Resilience Act (DORA) for the financial sector, published on 24 September 2020, the European Commission proposed provisions that set requirements for entities’ cyber security testing, including regular threat-led testing for entities designated, under the regulation, by supervisory authorities. It has also been proposed that, following consultation with the ECB and with consideration given to existing frameworks, the European Banking Authority (EBA), the European Insurance and Occupational Pensions Authority (EIOPA) and the European Securities and Markets Authority (ESMA) have been tasked with drafting regulatory technical standards for the testing framework. It is assumed that when the standards are set, DORA will be of relevance for the EEA and transposed into Norwegian law. This may entail a need for adjustments to TIBER-NO.

TIBER-NO is the first national implementation for red team testing of cyber security in the financial sector in Norway.

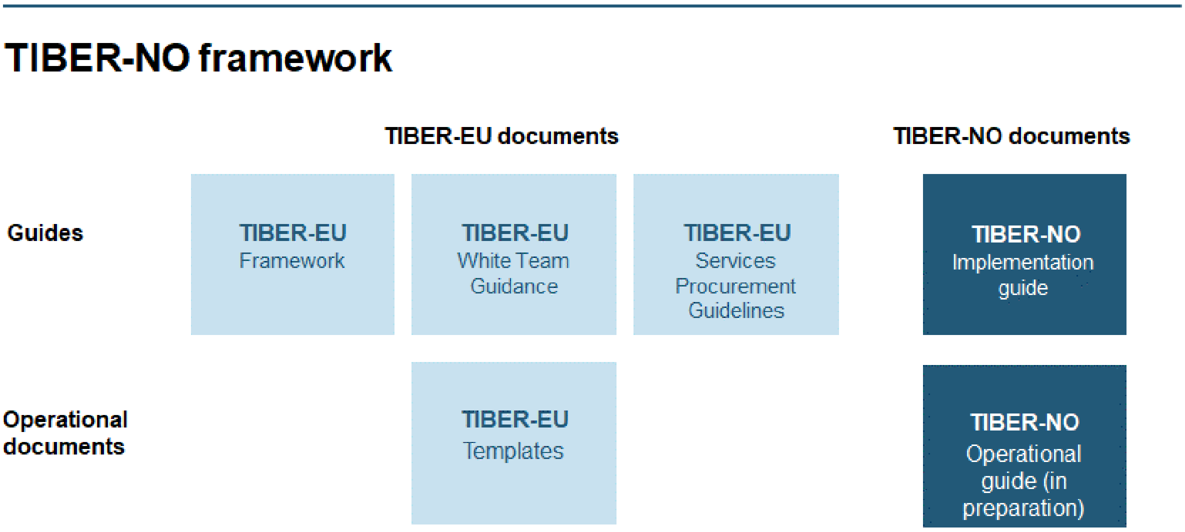
The TIBER-EU framework permits national implementation that accommodates national specificities. For TIBER-NO, the objective is to promote financial stability through greater cyber resilience of critical functions in the Norwegian financial system. Critical functions will be prioritised in the testing. TIBER-NO will not be introduced as a tool for the supervision or oversight of entities or individual financial market infrastructures/systems.

A number of large participants in the Norwegian financial sector are part of multinational corporate groups. An objective for TIBER-NO is to enable multinational corporate groups to test their activities in Norway in accordance with the framework.

TIBER-NO is primarily addressed to financial sector entities that are critical to the financial system in Norway. However, the choice has been made to allow non-critical functions to be included in TIBER-NO tests. This gives financial sector entities without critical functions the option of participating in TIBER-NO and conducting TIBER-NO tests, and gives entities with critical functions the option of including their non-critical functions in TIBER testing.[2]

In determining critical functions, criteria from the Single Resolution Board (SRB) will be taken into account.[3]

The TIBER-EU framework specifies the obligations for a TIBER test, including guidance and templates to be followed (Chart 1).



TIBER-NO framework

	TIBER-EU documents			TIBER-NO documents
Guides	TIBER-EU Framework	TIBER-EU White Team Guidance	TIBER-EU Services Procurement Guidelines	TIBER-NO Implementation guide
Operational documents		TIBER-EU Templates		TIBER-NO Operational guide (in preparation)

Chart 1: TIBER-EU and TIBER-NO guidance and operational documents

TIBER-EU framework gives relevant authorities in any jurisdiction the option to be adopted on voluntary basis. Moreover, it is up to the jurisdiction to determine which entities should undertake a test either on voluntary or mandatory basis. In Norway, the choice was made for participation in TIBER testing to be voluntary and as such any entity choosing to participate in

[2] Allowable under TIBER-EU and is also practiced in other jurisdictions
[3] https://www.srb.europa.eu/system/files/media/document/critical_functions_final.pdf

TIBER-NO will undergo TIBER tests. Entities choosing to participate in TIBER-NO will benefit from the experience of other TIBER tests of other entities in Norway and of tests in other jurisdictions. The entity tested "owns" the information from its own tests and decides what may be shared and with whom. Experience from other jurisdictions that have introduced TIBER shows that test results are normally shared at an aggregate (summary) level.

For TIBER-NO, emphasis is given to adapting TIBER testing to Norwegian conditions and the Norwegian financial sector. TIBER-NO has been developed by Finanstilsynet and Norges Bank in dialogue with the industry, with weight given to efficient use of resources, gradual implementation and learning and adapting the framework in the process.

1.4 Purpose of the guide

This implementation guide provides an overarching description of preconditions that must be met, including how TIBER-NO tests are to be conducted, in order for the test to be recognised as a TIBER test[4]. The guide describes how TIBER-NO is operationalised in Norway and provides an overview of requirements, processes and roles. The implementation guide is the core document of the Norwegian TIBER implementation.

For a full overview, the guide must be read together with documents from the TIBER-EU framework and the TIBER-NO *Operational guide*[5]. See the overview of relevant documents in Chart 1.

1.5 Legal basis and copyright

As part of the implementation of TIBER-EU in Norway and the preparation of this guide, Norges Bank has assessed the framework against Norwegian laws and regulations and EU legislation with EEA relevance. The purpose was to prevent conflicts in requirements, methodologies and processes between TIBER-EU and TIBER-NO. The assessment has been conducted on the basis that the formal responsibility for managing the TIBER-NO implementation guide is taken by Norges Bank.

The conclusion following the legal review is that the TIBER-EU framework can be implemented in compliance with Norwegian legislation. A key assumption for this conclusion is that all entities and institutions that participate in TIBER-NO do so on a voluntary basis.

The legal assessment will be re-reviewed and updated regularly to ensure that TIBER-NO continues to remain in compliance with Norwegian legislation. Such updates will be performed as long as the framework is in use in Norway.

It is the responsibility of the entities and third-party providers tested in a TIBER test to ensure that they conduct the test in accordance with all laws and regulations and that appropriate risk management and controls are in place.

[4] The guide has been developed jointly by Finanstilsynet and Norges Bank and is published on the two entities' websites.

[5] The TIBER-NO *Operational guide* is in preparation.

The entities participating in TIBER-NO are responsible for conducting a legal review before testing is carried out, and may not rely on the legal review performed by Norges Bank.

The *Implementation guide* (this document) is only intended to provide general information about TIBER-NO. The information in the guide cannot be regarded as legal or operational advice. The document contains elements taken from the publication TIBER-EU Framework: How to implement the European framework for Threat Intelligence-based Ethical Red Teaming, to which the ECB holds the copyright.

2 Roles and responsibilities in TIBER-NO

2.1 TIBER-NO Cyber Team (TCT-NO)

Finanstilsynet and Norges Bank are collaborating on the implementation and adoption of the TIBER-EU framework in Norway and will establish the necessary forums for overarching compliance monitoring, governance and involvement of industry representatives and other relevant authorities. The assessment of what constitute critical functions and the overall determination of the entities and functions to be tested are the responsibility of Finanstilsynet and Norges Bank via these fora.

Norges Bank is responsible for the organisation and resourcing of the TIBER-NO Cyber Team (TCT-NO), which will manage and operationalise TIBER-NO, and has the formal responsibility for managing the TIBER-NO implementation guide.

The TCT-NO should have the requisite experience and knowledge of the types of ICT operations of entities that shall potentially be tested. Furthermore, the TCT-NO must have knowledge about relevant ICT systems, risk management expertise, knowledge of threat actors' motives and objectives, tactics, techniques and procedures (TTP), and expertise in geopolitical and threat developments. The TCT-NO must have the expertise needed to review and approve all material prepared in the test process.

The TCT-NO is responsible for overseeing all TIBER-NO tests to ensure compliance with TIBER-NO. The TCT-NO will ensure that the critical functions in the financial system are tested and included in the scope of entities being tested.

The TCT-NO follows up TIBER-NO tests to ensure that they satisfy the requirements of the TIBER-EU framework and that they can be recognised as TIBER tests; TCT-NO can and should provide advice and recommendations on the scope for tests, and has the right to invalidate a TIBER test if the test is not performed in accordance with the requirements of TIBER-NO.

The TCT-NO ensures that entities conduct tests in a uniform and controlled manner. The TCT-NO cannot be held liable for the actions of entities' White Team, the entity itself or providers to the entity, or for any effects or consequences that the TIBER-NO test has had for the participating entity or a third party.

The TCT-NO is responsible for regular updates of the TIBER-NO implementation guide as tests are conducted and other experience is gained, and as changes are made to TIBER-EU. The TCT-NO maintains the TIBER-NO implementation guide in collaboration with entities participating in TIBER-NO and TCTs in other jurisdictions.

The TCT-NO participates in the TIBER Knowledge Centre (TKC), operated by the ECB.

2.2 Generic threat landscape report

A generic threat landscape (GTL) report is an overall assessment of the threat scenarios facing financial institutions. The GTL report forms the basis for the targeted threat intelligence (TTI) reports prepared and used for TIBER tests.

The TCT-NO is responsible for the preparation, maintenance and regular updates of the GTL report for TIBER-NO. Nordic Financial CERT (NFCERT) prepares a Nordic GTL report with national appendices describing the financial sector threat landscape. This report is updated at least once a year. Nordic countries that have adopted TIBER-EU have decided that the NFCERT GTL report will be the GTL report for TIBER testing and has also been chosen for TIBER-NO.

The TCT-NO shall ensure that relevant organisations[6] are sufficiently involved in the preparation of the GTL report for TIBER-NO, and that the report is shared with other entities participating in TIBER-NO. The TCT-NO is also tasked with helping to quality assure the contents of the GTL report.

The GTL report assesses how threats from state actors, economic criminals, activists and other threat actors can affect critical functions of financial institutions, other key participants in the banking and payment system and their key providers. The GTL report addresses the motives and objectives of threat actors, and the tactics, techniques and procedures (TTPs) they use in their attacks.

2.3 Collaboration with other parties and information sharing

In collaboration with the TCT-NO and others, NFCERT is responsible for preparing the GTL report, which is an important basis for all TIBER-NO test planning. While preparing the report, NFCERT is in dialogue with relevant national authorities in the area of cyber security.

The GTL report may be shared with relevant threat intelligence and red team providers, both those that have and have not provided previously under TIBER-NO, and with entities that have not yet been tested.

NFCERT supports member entities’ response to cyber attacks and thus also entities’ response to cyber attack simulations as part of a TIBER test. At meeting forums established outside TIBER-NO, NFCERT shares its summaries of attacks (where it has supported entities) with relevant national authorities in the area of cyber security.

The entity tested is the legal owner of all the material produced during the test. The entity shares test results with the TCT-NO[7]. The TCT-NO will share test information with others only if the entity gives its consent.

The TCT-NO does not have a supervisory or oversight role over individual systems and/or entities. The TCT-NO shall not share TIBER-NO information about the tests or other documentation about tested entities without the consent of the entity. The organisation of the TCT shall help to ensure

[6] For example NCSC, NC3 and Nordic Financial CERT

[7] See Sections 4.4.1 (Remediation planning) and 4.4.2 (Result sharing) for more information on the tested entities’ sharing of test results with the TCT-NO.

that TIBER-NO tests can be conducted in a transparent and collaborative manner without imposing upon tested entities a statutory requirement as a direct result of the testing, and outside the purview of ordinary supervisory and oversight activity. When a TIBER-NO test with test report is completed, the TCT-NO informs the Norwegian supervisory and oversight authorities that the entity's testing has been completed.

As part of their ordinary supervisory and oversight activities, supervisory and oversight authorities may request information about TIBER testing from individual entities directly, so long as they are authorised to do so. To secure transparency in the oversight and supervision of an individual institution, Norges Bank and Finanstilsynet will only obtain information about TIBER tests for this purpose directly from the individual entity tested. In line with the main purpose of TIBER-NO, information obtained from the TCT-NO can be used by the two institutions in a system perspective, for example for assessments of financial stability, although then only as a basis for the assessments. Norges Bank and Finanstilsynet will prepare guidelines and routines for sharing information between and within the two institutions.

2.4 International collaboration

One of the objectives of TIBER-EU is to standardise and harmonise threat intelligence-based red team testing in order to facilitate cross-border TIBER-EU testing of multinational entities. To achieve this, TCTs in all countries that have adopted TIBER-EU are responsible for contacting other relevant TCTs when a test entails a need for testing in several countries.

Prior to each TIBER-NO test, the TCT-NO, along with the entity to be tested, shall identify whether the test covers testing in other countries. If it does, the TCT-NO contacts the TCTs in these countries with the aim of establishing a collaboration on the testing and mutual recognition of the test.

Likewise, the TCT-NO can, upon request, enter into a collaboration with authorities (TCTs) in other jurisdictions when testing of entities domiciled in another jurisdiction entails a need for testing under TIBER-NO.

TIBER testing collaboration involving Norwegian entities requires the consent of the Norwegian entity.

3 Stakeholders in the TIBER-NO test process

Stakeholders directly in a TIBER-NO test are:

- Norges Bank
- Finanstilsynet
- The TIBER-NO Cyber Team (TCT-NO)
- The entity to be tested, organised in a White Team (WT) and a Blue Team (BT)
- Third-party providers of threat intelligence (TI) and red team (RT) testing
- Nordic Financial CERT (NFCERT)

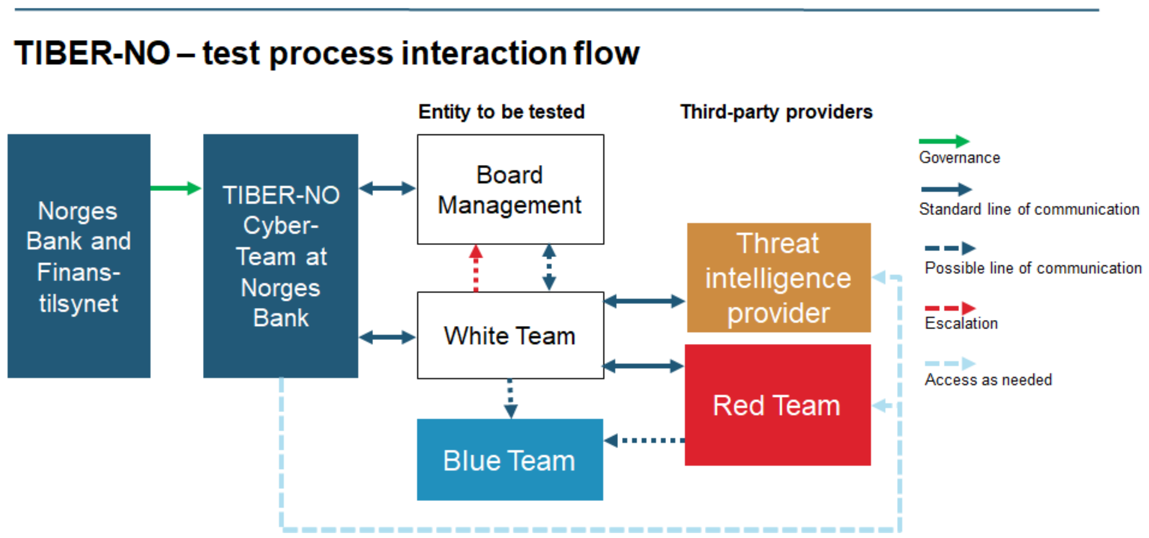

TIBER-NO – test process interaction flow
Entity to be tested
Third-party providers
Norges Bank and Finans-tilsynet
TIBER-NO Cyber-Team at Norges Bank
Board Management
White Team
Blue Team
Threat intelligence provider
Red Team
Governance
Standard line of communication
Possible line of communication
Escalation
Access as needed

Chart 2: Actors in a TIBER-NO test with expected communication flows

NFCERT will support the entity being tested in the same manner as in a real-life attack.

Under TIBER-EU, it is optional for national adaptations to require, if necessary, involvement of national intelligence agencies, cyber security centres or relevant police units. TIBER-NO has not set requirements for such participation.

3.1 Organisation and management of TIBER tests.

Entities that undergo TIBER-NO tests are themselves responsible for managing and organising the test. This includes procuring external providers, performing risk management, implementing controls, processes and procedures to ensure that the test complies with requirements in the TIBER-EU framework and also follows best practices.

3.1.1 White Team (WT)

For each TIBER-NO test, the entity to be tested must set up a White Team (WT). On behalf of the entity, the WT is responsible for determining the scope of the test and conducting it, communicating with the other participants and risk management during the test.

The WT should be staffed by managers and other employees of the entity that are knowledgeable about the entity’s critical functions and the systems that underpin them. The WT should not comprise more persons than necessary, and the number of persons within the entity with knowledge of the test should be kept to a minimum. The WT is responsible for ensuring that planning and heading the test comply with TIBER-NO.

The WT is to have its own leader, the White Team Lead (WTL). The WTL coordinates all testing activity, including handling TI and RT providers.

More information about roles, responsibilities and composition of the WT is available in TIBER-EU White Team Guidance.

3.1.2 Blue Team (BT)

All managers and other employees of the entity who are not a part of the WT are to belong to the Blue Team (BT). It is important that all members of the BT are excluded from the preparation and conduct of the TIBER-NO test and have no knowledge whatsoever of the content and duration of the test.

In the closure phase when the test results are reviewed, the WT shall inform the BT. Relevant representatives of the BT should participate in the review and follow-up of the test result.

3.1.3 Third-party providers

TIBER-NO tests require the use of independent third-party providers of both threat intelligence and red team testing. According to TIBER-NO, a test can only be approved if it is conducted by external threat intelligence and red team providers.

Even though tests conducted by internal red teams provide value and should as a rule be performed as a good practice, there are clear advantages to having external RT providers. External providers have a more independent perspective; as internal teams on the other hand are often linked to internal systems, people and processes and possess the expertise that is not available to external teams, nor to threat actors. Furthermore, external providers often have more resources and up-to-date skills to deploy and provide a fresh perspective that may test scenarios the internal team has omitted.

A successful implementation of TIBER-NO testing, including managing risks, requires that TI and RT providers are competent, qualified and have the requisite experience. The TIBER-EU Services Procurement Guidelines can be helpful in this regard.

As part of the procurement of TI and RT providers, the following are to be included in the agreement: the test's scope and restrictions, risk-reduction measures related to conducting the test, timing, availability of providers, contracts and liability.

3.1.4 Targeted threat intelligence (TI) providers

The threat intelligence (TI) provider is an external service provider procured by the WT. The TI provider gathers targeted intelligence on the entity to be tested which corresponds with information a sophisticated cyber attacker would have access to, and presents this information to the entity in the form of a targeted threat intelligence (TTI) Report. It is recommended that the providers use a number of sources in addition to the GTL report in their intelligence gathering in order to compile a TTI report that is as accurate and up-to-date as possible. The White Team is the recipient of the report and should vet the report.

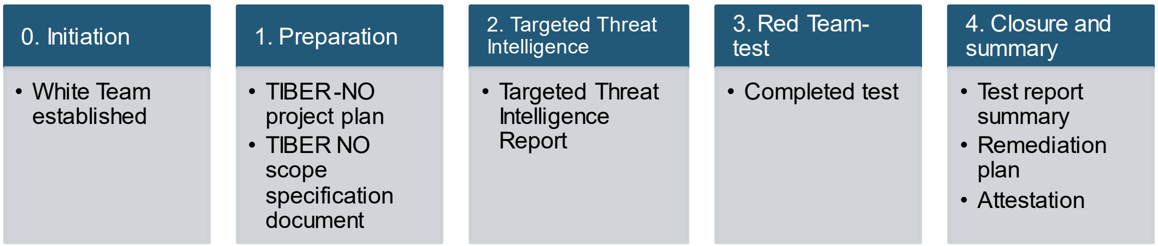
3.1.5 Red Team (RT)

Red team testing is provided by an external service provider, a red team (RT) provider procured by the White Team. The RT provider will attempt to "break in" to the entity's ICT systems with the aid of ethical hacking methodologies and tools following the threat intelligence provided in the TTI report. The RT provider shall follow strict ethical guidelines at all times. The RT plans and carries out a TIBER-NO test of systems and services based on the scenarios developed by the TI provider. After the test, the RT compiles a report documenting findings identified by the test.

Internal resources within the entity being tested may, by agreement with the provider and approval of the TCT-NO, participate in the test and support the external RT provider. Such participation requires written agreement between the RT provider and the entity.

4 TIBER-NO test process

Chart 3 provides an overarching description of the phases of a TIBER-NO test, including deliverables for each phase.



0. Initiation	1. Preparation	2. Targeted Threat Intelligence	3. Red Team-test	4. Closure and summary
• White Team established	• TIBER-NO project plan • TIBER NO scope specification document	• Targeted Threat Intelligence Report	• Completed test	• Test report summary • Remediation plan • Attestation

Chart 3: The phases of a TIBER test with results for each phase

4.1 Initiation phase

Entities participating in TIBER-NO are provided with templates, guides and other relevant TIBER-NO and TIBER-EU documentation by the TIBER-NO Cyber Team (TCT-NO).

A TIBER test of an entity participating in TIBER-NO may be initiated by the TCT-NO or the entity itself. Once it has been determined that an entity will conduct a TIBER test, the TCT-NO will prepare a draft overall plan with milestones. Then the entity begins its planning. An important part of planning is to identify stakeholders beyond the TCT-NO and third party service providers[8] to be involved. Critical service providers, including data centres are examples of such stakeholders.

The entity's internal organisation for conducting the TIBER-NO test, the White Team (WT), is established in the initiation phase. This introductory phase also includes market surveys to identify third-party service provides and identify legal issues that need to be clarified prior to testing.

In the initiation phase, the entity performs an initial assessment of the critical functions to be included in the test (scoping) and the ICT systems that support them. The assessment is based on the overarching critical functions that the TCT-NO believes should be tested and the critical functions in the entity's organisation that support them.

4.2 Preparation phase

In the preparation phase, the TIBER Test Manager (TTM)[9] engages in a dialogue with the entity to be tested to formally start the project. This phase should be initiated at least three months prior to the actual test.

[8] In this context, third-party service provider means threat intelligence (TI) provider and Red Team (RT) provider.

[9] The TTM is a part of the TCT-NO.

The TCT-NO and the entity shall agree on the scope of the test, and the entity is to procure the cyber security service provider(s). This phase is normally expected to take four to six weeks, excluding the entity's procurement process.

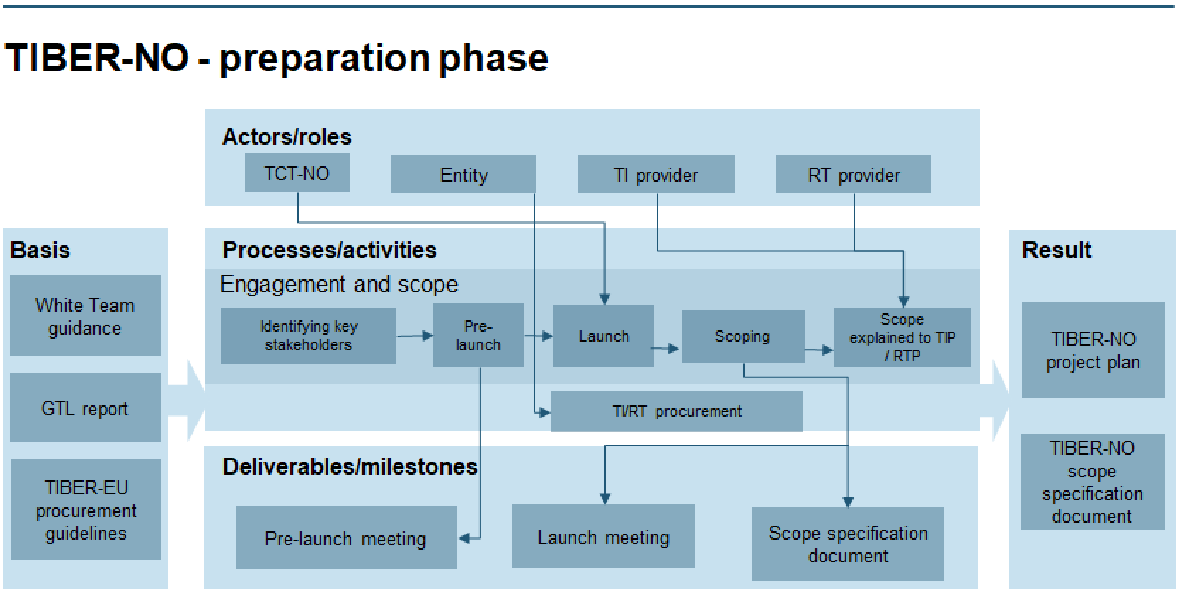


Chart 4: Preparation phase with actors, activities and deliverables

4.2.1 Preparation meetings

The preparation phase starts with a meeting (pre-launch meeting) between the TCT-NO and the White Team (WT). At this meeting, the TCT-NO will inform the entity of requirements of the TIBER-NO process, stakeholder roles and responsibities, security protocols and contractual considerations relating to TI and RT providers. Furthermore, the TCT-NO will ensure that the WT begins its preparations and that a WTL is appointed. This includes overarching project planning in line with the agreed dates, procurement of third-party providers, risk management and scoping for the test. A final decision on the scope may be taken later (see Section 4.2.2).

The entity should start the procurement process immediately after the pre-launch meeting.

Later in the preparation phase, a meeting shall be conducted involving all stakeholders in the TIBER-NO test (launch meeting; see chart above) at which the stakeholders clarify their expectation and review the test process. On the background of this meeting, the WT prepares the draft TIBER-NO project plan.

4.2.2 Scoping

The scope of the test and the critical functions to be tested must be determined on the basis of the assessment of the scope performed in the initiation phase (4.1). The entity to be tested assesses the internal functions that support critical functions to be tested and clarifies this with the TCT-NO. The WT and TI/RT providers participate in this determination.

The scope of the test is documented by the WT in the entity to be tested in the TIBER-EU scope specification document, which sets out the scope of the TIBER test and lists the key systems and services that underpin each. This helps the WT to set the "flags" to be captured and define more overarching objectives for the test. Although the flags are set during the scoping process, they can be changed in subsequent phases, e.g. on the basis of updated information following threat intelligence gathering or testing (as the red team test evolves).

The TCT-NO is responsible for ensuring critical functions are tested in an appropriate manner to secure financial stability. The TCT-NO verifies the scope of the test conforms to the TIBER-NO and gives its approval. TCT-NO may request the oversight and supervisory authorities to assist in the scoping of the test.

The scope will have to be agreed at the board level of the entity to be tested. Access to information about the test should be limited as much as possible.

4.2.3 Services procurement

According to TIBER-NO, a threat intelligence-based test may be recognised as a TIBER-EU test only if it is conducted with the aid of independent third-party service providers.

Two types of third-party service providers must be involved:[10]

- The Threat Intelligence (TI) provider delivers a targeted threat intelligence report (TTIR), which describes relevant threat actors and proposed threat scenarios for testing.
- The Red Team (RT) provider performs the attack on the agreed systems and services "scoped into" the test according to the TTIR. After the test is carried out, the RT provider then delivers a description of the test, including any problems with implementation and a Red Ream test report, to the entity.

The entity is responsible for making sure that there is a mutual agreement between the TI and RT providers on at least the following aspects: the scope of the test; boundaries; timing and availability of personnel, contracts, agreed control actions and testing; and a liability clause and relevant insurance. The contracts should include:

- a requirement to meet security and confidentiality requirements at least as stringent as those followed by the underlying entity;
- indemnification of personnel involved in the test;
- a clause related to data destruction and breach notification provisions;
- activities that are not allowed during the test, such as: destruction of equipment; uncontrolled modification of data/programs; jeopardising continuity of critical services; blackmail; threatening or bribing employees; and disclosure of results.

The entity to be tested is responsible for ensuring that the providers chosen meet the minimum requirements TIBER-EU Framework Services Procurement Guidelines.

4.2.4 Risk management

The TIBER-NO test takes place in the financial institutions' and/or their related service providers' ICT production environments and therefore entails elements of risk for these entities. The WT is responsible for implementing appropriate risk-reduction controls, processes and procedures to

[10] One provider can deliver both services, in a given test

ensure that the test is carried out with due consideration and that risk is at the entity's accepted level.

Risk is to be identified, analysed and managed (including reduced, avoided, transferred or accepted) in accordance with the entity's risk management framework and practices. Risk assessment and implementation of measures to manage risk must be completed before testing begins. This is the responsibility of the WT.

When the preparation phase is completed, the entity will have produced:

- *TIBER-EU scope specification document*, which sets out the scope of the test and chosen TI and RT providers.
- *TIBER-NO project plan.*

4.3 Testing phase

4.3.1 Targeted threat intelligence

The purpose of this phase is to ensure that the test is intelligence-led, i.e. based on the entity's real-life threat landscape. The threat landscape includes relevant threat actors, their objectives and how they operate. Intelligence is gathered, structured and presented in a targeted threat intelligence report (TTIR).

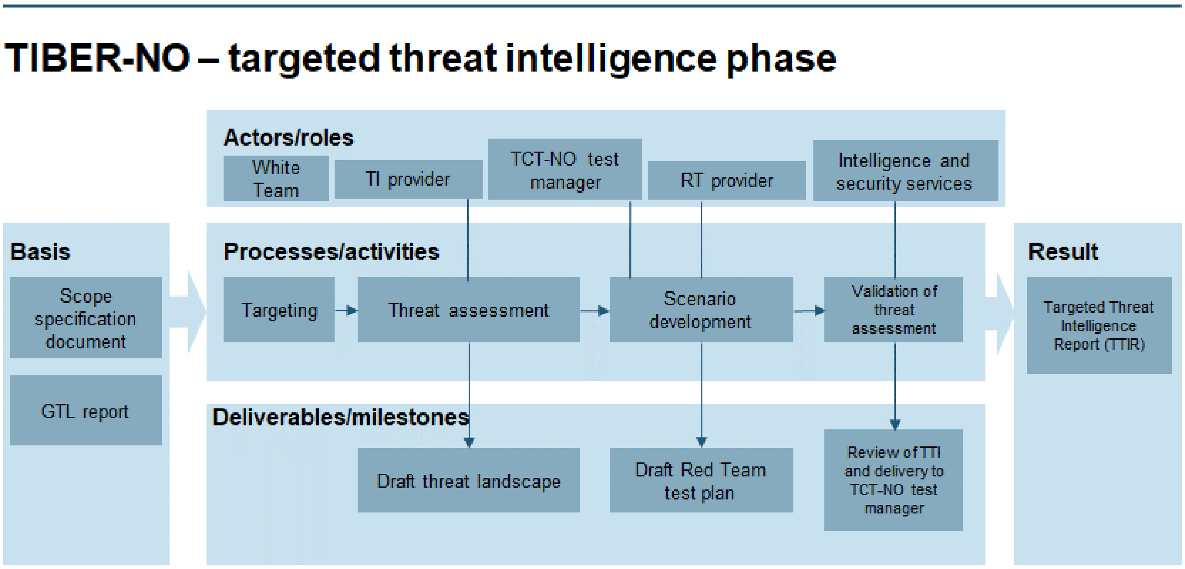

TIBER-NO – targeted threat intelligence phase
Actors/roles
White Team
TI provider
TCT-NO test manager
RT provider
Intelligence and security services
Basis
Scope specification document
GTL report
Processes/activities
Targeting
Threat assessment
Scenario development
Validation of threat assessment
Result
Targeted Threat Intelligence Report (TTIR)
Deliverables/milestones
Draft threat landscape
Draft Red Team test plan
Review of TTI and delivery to TCT-NO test manager

Chart 5: Targeted threat intelligence phase – actors, activities and deliverables

The TTIR describes realistic attack scenarios targeting the entity's critical functions that can be included in the test. Prior to this phase, the entity should have provided relevant information to the TI provider to enable it to prepare the TTIR. This information should contain a business and technical overview of each critical function-supporting system, the entity's current threat assessment and threat register and examples of recent attacks on the entity.

The GTL Report is submitted to the TI provider, which uses it as the basis for identifying specific threat actors relevant for the test.

The TI provider is responsible for gathering targeted intelligence from a broad range of sources[11]. The TI provider then analyses the information and submits a draft TTIR, after which the TI provider develops scenarios with relevant threat actors and probable scenarios for the specific entity. The TI provider produces a draft test plan.

The final product of this phase is a TTIR, which contains three parts.

The first part is an overview of the entity from an intelligence perspective. The overview is intended to help to create a strategic understanding of the business areas with current and planned activities. This part should provide insight into business and system consequences if critical functions are compromised. To make this process as efficient as possible, the entity should furnish the TI provider with the following information:

- A description of the entity's core functions, including underlying factors that are critical to these core functions and an explanation of why the entity is critical to the financial system.
- A business and technical overview of each critical function-supporting system covered by the test (in scope).
- The current threat assessment and threat register.
- Examples of related recent threats.

The second part is an overview of actors and overarching scenarios. In this part, the GTL report will be broken down by the TI provider to be more specific to the entity to be tested. An assessment is made of the intentions and capabilities of relevant threat actors to attack the entity and its critical functions. The analysis should conclude with a list of the most probable and capable threat actors.

In the second part, the TI provider will devise several overarching scenarios for how an attack by the selected threat actors can behave. The scenarios should be linked to the threat actors' motivations and intentions to attack the specific critical functions. The report should contain:

- The most relevant threat actors for attacking the entity's critical functions.
- An account of threat actor motivations in order to provide an insight into their possible motives for attacking.
- Most probable targets for each threat actor.
- Overarching attack scenarios for each threat actor.

Part three of the report is intelligence on the entity's digital presence (attack surface). In this part, the TI providers will provide the Red Team with intelligence on what the relevant threat actors are able to discover about the entity's potential attack surfaces. The purpose is to be specific about the opportunity space for threat actors. The entity's WT can provide information to the TI provider to focus the search.

Wherever appropriate and relevant, it is desirable that national intelligence and security services (agencies) will vet the report before the TTIR is delivered to the TTM.

[11] Including open sources, e.g. OSINT, TECHINT and HUMINT.

Under TIBER-NO, the TI provider for a particular test has the option of continuing the engagement while the test is being conducted and delivering updated intelligence in this period as required.

4.3.2 Red team test

This phase begins when the TI provider submits the targeted threat intelligence report (TTIR) to the RT provider. The report describes the proposed threat scenarios for the test.

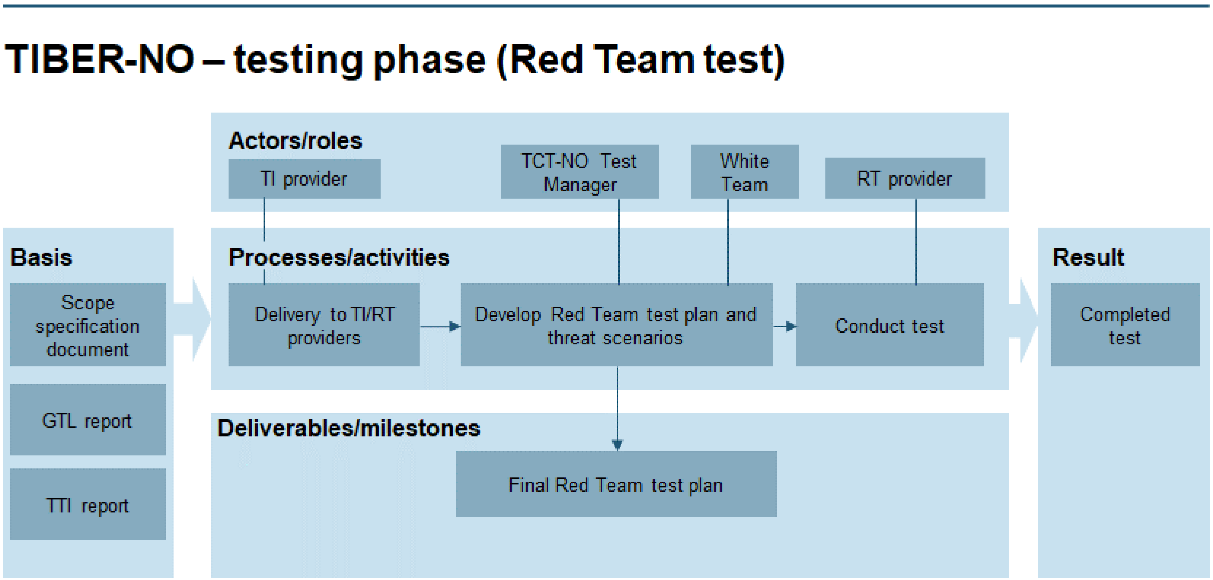


Chart 6: Testing phase with activities, actors and deliverables

The RT provider uses the scenarios in the TTIR as the basis for further development. This is to be done in a way so that they remain threat intelligence-driven. As a part of this planning, the RT provider proposes the specific objectives to be achieved in the test.

The entity to be tested provides feedback on the RT provider’s proposed attack scenarios with the help of the WT and makes the final decision on the scenarios to be tested. On the basis of these scenarios, the RT provider conducts a test of specific production systems, employees and processes in the entity’s critical functions. The RT provider should use a number of techniques, tactics and procedures in the course of the test.

The RT provider must follow strict ethical guidelines at all times. The test is to be conducted in a controlled manner for all scenarios to be tested. Testing must not entail unnecessary risk for the entity being tested or its critical functions or for other parties dependent on services provided by the entity. The entity being tested may, with the aid of the WT, immediately put scenarios on hold if other significant events occur.

The time allotted to the test should be proportional to the scope of the test. Based on experience, the testing phase of most TIBER tests is expected to be around 10-12 weeks (10 weeks being the minimum). This is only an estimate. The time spent will vary depending on entity size, scenarios chosen, test scope, including critical functions to be tested, and other factors.

TIBER-EU gives individual countries the option of allowing the use of physical attack vectors such as various physical objects, including flash drives and devices connected to wireless networks etc. and plant these objects in order to gain access to the internal computer network. It should be emphasised that the risk assessment prior to each test must include a thorough assessment of the use of such objects.

In addition to the predefined scenarios, the RT provider may propose additional scenarios after the test has commenced to make the test even more realistic, “Scenario X”. This enables the RT provider to propose new ways to reach the objective, based on experience and knowledge acquired during the test. Any use of Scenario X must be approved by the WT and TCT-NO.

4.4 Closure phase

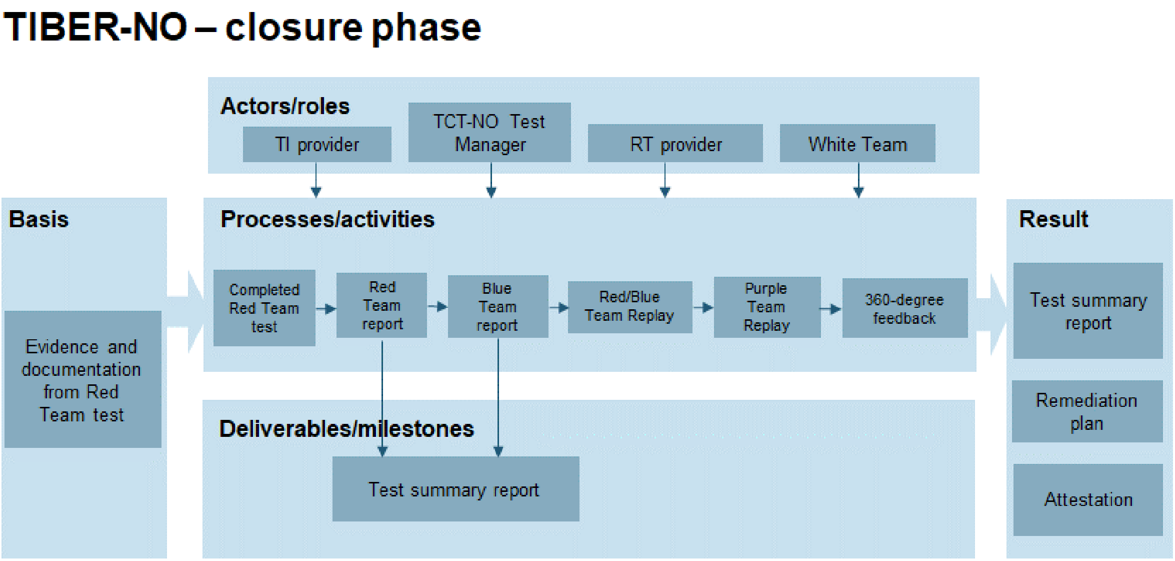


Chart 7: Closure phase with activities and deliverables

During the closure phase, the RT provider prepares a test report, which describes testing, findings and observations. The report should contain recommendations for measures to improve technical controls, policies, procedures and routines, and if necessary, advice on improving skills or tightening access to relevant information in the entity’s organisation. The report is delivered to the entity’s WT. The entity’s Blue Team (BT) is informed by the WT about the test and the scenarios tested. The report is shared with the TCT-NO.

Learning is an important purpose of a TIBER test. “Purple teaming” and 360-degree feedback meetings can contribute to such learning and are optional activities under TIBER-NO. Purple teaming involves bringing together the RT and BT for a joint summary and experience transfer session.

It is optional for the TCT-NO, oversight body, supervisory authority and TI provider to be invited to joint summary meetings to be conducted after the completed test. The White Team Lead (WTL) decides who should be invited.

4.4.1 Remediation planning

Once the review of the test results is completed, the entity tested is responsible for processing the test findings and preparing a test summary report and remediation plan.

The test summary report is intended to provide a picture of the overall test process with the test results. The report is written on the basis of reports from the BT, RT, respectively, and the TTI report. The test summary report must not contain detailed technical information or specific information on weaknesses and vulnerabilities in the findings. Information at such a detailed level is potentially highly sensitive information that belongs to the entity tested and should not be shared. The entity is responsible for sharing an aggregated version of the test summary report with the TCT-NO. The TCT-NO may review the more detailed findings from the test with the entity at the entity's request.

The Remediation plan is based on the test results and should be used for making improvements in the entity's organisation.

4.4.2 Result sharing

Once the test reports have been completed, the entity tested, the TI/RT providers and the TCT-NO should provide an attestation confirming that the test was conducted in accordance with the TIBER-NO implementation guide. The attestation should be signed by the board of the entity tested and by the TI/RT providers. The attestation approves the completed test as a TIBER test for recognition by other relevant authorities, including TCTs in other countries.

The draft test summary report, which describes the overall test, with the process, results and remediation plan, should be shared with the TCT-NO, so that the TCT-NO has the opportunity to comment before the report is finalised. The TCT-NO will analyse the test results, identifying findings, threats and vulnerabilities. The TCT-NO may share its assessments and analyses – at a suitably aggregated level – with other entities participating in TIBER-NO. Before the TCT-NO can share assessments, this must be approved by the entity tested for each test.

One of the main objectives of TIBER-NO is to strengthen financial sector resilience to cyber incidents. Therefore, the TCT-NO will, whenever relevant, analyse the results of tests in other jurisdictions to identify key findings and common threats and vulnerabilities. TCT-NO will share this with relevant TIBER-NO stakeholders within the current guidelines. Such sharing must be approved by the entity being tested.

TCT-NO is able to share anonymised findings and learnings from TIBER tests in Norway with the TIBER Knowledge Centre (TKC). This enables the TKC to assemble key findings and obtain a picture of the resilience of the European financial. All exchange of information between the TCT-NO and the TKC should be done in a secure manner.

4.5 Interactions during a TIBER-NO test

All parties involved in a TIBER-NO test are responsible for working together in a collaborative, transparent manner and for effective implementation. Essential for a successful test is a close working relationship between the WTL and the TCT-NO in all phases of the test. A number of key features of a sound collaborative approach appear below.

Responsibility for overall planning and leadership of the test rests with the tested entity. The WTL is responsible for the scope, scenarios and management of risks associated with the test and for ensuring that the test is recognised and validated by the TCT-NO. The WTL is tasked with coordinating all test activity, including the engagement of third-party providers. The WTL should ensure that providers' project plans are an integral part of the entity's overall planning of the test. The scope of a TIBER-NO test must be approved by the entity's board or executive management.

In the closure phase, the WTL is responsible for involving relevant actors in the entity's organisation (including Blue Team Lead) to a joint review and follow-up. If there have been deviations in the conduct of the test from the original plan, the deviations should be discussed with the TCT-NO.

Even though the WTL is the primary contact point for an entity's third-party providers, the TCT-NO should also be in direct contact with these providers. Whenever important decisions are to be made (e.g. in the event of deviations from the agreed scope during the test) or where conflicts of interest arise, both the WTL and TCT-NO should follow escalation routines in their own organisations to their respective superiors.

Appendix 1 – Abbreviations used in this guide

BT	Blue Team: entity’s security or response capability, with no knowledge of the test
DORA	Digital Operational Resilience Act for the financial sector
EBA	European Banking Authority
ECB	European Central Bank
EIOPA	European Insurance and Occupational Pensions Authority
ESMA	European Securities and Markets Authority
GTL	Generic threat landscape: report on cyber threats targeting the financial sector in Norway used as the basis for planning TIBER tests
NFCERT	Nordic Financial CERT
RT	Red Team: team that performs the security (penetration) testing
RT provider	Red team (RT) provider: security test provider that performs the penetration test
TCT-NO	TIBER-NO Cyber Team: group that administers and proposes changes to TIBER-NO, provides test support and is in contact with the ECB
TIBER	Threat Intelligence-Based Ethical Red teaming: threat-based testing performed with the aid of external “red team”-providers
TIBER-EU	Common European framework for threat intelligence-based ethical red team-testing under the auspices of the ECB
TIBER-NO	The national TIBER adaptation in Norway
TKC	TIBER Knowledge Centre: forum for knowledge sharing by national TIBER authorities, operated by the ECB
TTM	TIBER Test Manager: responsible for managing individual TIBER test (member of the TCT-NO)
TTIR	Targeted Threat Intelligence Report: threat intelligence report prepared prior to each test
TI provider	Threat Intelligence Provider: provider of bespoke threat intelligence for a specific TIBER test
TTP	Tactics, Techniques and Procedures used by real-life threat actors
WT	White Team: group familiar with and responsible for testing in the organisation of the entity being tested
WTL	White Team Lead: responsible for the White Team’s test management

Change log

Version	Change	Date	Approved by
1.0.1	Minor clarifications	2022.10.24	Steering group
1.0.0	Initial version	2021.09.29	Hovedstyret