OESTERREICHISCHE NATIONALBANK
EUROSYSTEM

TIBER-AT Implementation Guide

Sicherheit durch Stabilität

November 2023

Publisher and editor
Oesterreichische Nationalbank
Otto-Wagner-Platz 3, 1090 Vienna, Austria
PO Box 61, 1011 Vienna, Austria
www.oenb.at
oenb.info@oenb.at
Phone: (+43-1) 40420-6666

Printing and production *Oesterreichische Nationalbank, 1090 Vienna*

Data protection information *www.oenb.at/en/dataprotection*

ISSN 2309–3323 (online)

Printed according to the Austrian Ecolabel guideline for printed matter.

Please collect used paper for recycling. *EU Ecolabel: AT/028/024*

Inhalt

1 TIBER-AT in a nutshell

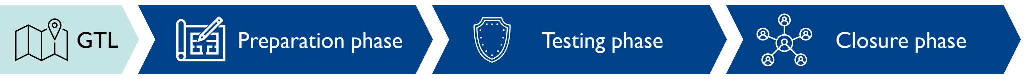
TIBER-AT is based on the TIBER-EU framework, a cybersecurity testing framework developed by the European System of Central Banks (ESCB). TIBER stands for "Threat Intelligence-Based Ethical Red Teaming" and focuses on simulating realistic cyberattacks. In contrast to most other respective methodologies, TIBER-EU provides for real life tests of operational critical systems without a separate test environment. Consequently, the tests are conducted under strict safety provisions. The tested Financial Entity (FE) takes all necessary measures to ensure that no risks arise for the FE or its customers. Essentially, TIBER-AT is aimed at continuously improving the cyber resilience of the Austrian financial sector. Participation is voluntary as a rule and not based on a pass/fail concept; the tests are in fact designed to bring maximum benefit to the FE. Admission for voluntary TIBER-AT tests will be coordinated with the TIBER Cyber Team Austria (TCT-AT).

However, under the new Digital Operational Resilience Act (DORA), Threat-Led Penetration Testing (TLPT) will be mandatory for specific FEs as of January 2025, whereby TIBER-EU will be the relevant standard. A TLPT conducted in accordance with TIBER-EU and the TIBER-AT Implementation Guide will therefore meet all respective DORA requirements. TIBER-AT will be updated towards the end of 2024 to ensure full alignment with DORA and respective regulatory technical standards for TLPT expected to be published by the European Supervisory Authorities in the second half of 2024.

According to the TIBER-EU framework, the FE is responsible for testing its own systems. Hence, the costs for a TIBER-AT test are borne by the FE, requiring them to put in place adequate budgetary arrangements.

Figure 1

Overview of TIBER-AT phases



Source: OeNB.

The test framework foresees *three main phases*. In the *preparation phase,* the FE sets up the project structure for the test, defines the test scope and procures external service providers for the next phase. The *testing phase* involves the gathering of Targeted Threat Intelligence (TTI). The TTI serves as the foundation for the external Red Team (RT) to conduct the simulated cyberattack using Tactics, Techniques and Procedures (TTPs) of real-world attackers. In the *closure phase* all involved parties document details of the exercise and translate the findings into a Remediation Plan to improve the FE's cyber resilience. Prior to the first phase of the test, the FE receives from OeNB and FMA a *Generic Threat Landscape (GTL)* report, which highlights the current threat situation for the Austrian financial sector and acts as a starting point for the FE-specific TTI Reports.

The TIBER-EU framework has already been adopted by most EU jurisdictions. The European Central Bank (ECB) has established the *TIBER-EU Knowledge Center (TKC)* for national authorities, that oversees and supports consistent national implementation of the TIBER-EU framework. *TIBER-AT* implements the TIBER-EU framework for the Austrian financial sector, includes all mandatory elements of TIBER-EU and deals with certain national specificities.

2 Target audience

TIBER-AT is targeted at *FEs* that are *critical* for the functioning of the financial sector. The aim is to strengthen their cyber resilience and reduce potential contagion effects in the financial sector. In accordance with DORA, the following entities are addressed:

- *Large credit institutions* licenced in Austria
- *Large insurance companies* licenced in Austria
- Major *financial market infrastructures* operating in Austria

TIBER-AT focuses on FEs in which the failure of critical functions (CFs) or services could lead to systemic disruption or lasting negative consequences for the financial sector, financial stability, public security or other equally critical areas. The FE shall take the necessary measures to enable the participation of ICT third-party service providers to the extent that they support or provide critical functions of the FE under TIBER-AT. For the time being, the target group has deliberately been defined loosely to allow for a case-by-case assessment of the suitability of TIBER-AT to the FE.

Participation in a TIBER-AT test requires a *certain level of cyber maturity.* The full benefit of such a test only unfolds when gross deficiencies and weaknesses have already been addressed so that the focus can be shifted to the detection of more intricate FE-specific vulnerabilities.

3 Main parties involved in a TIBER-AT test

Due to the broad scope and complexity of cybersecurity testing, a TIBER-AT test involves multiple stakeholders. The close cooperation and open collaboration between these stakeholders are key to the success of the test. For an overview table of the stakeholders' roles throughout the test see Appendix 6.1.

3.1 White Team (WT)

The White Team (WT) is the central hub for the TIBER-AT test within the FE and is headed by the White Team Lead (WTL), who is appointed by the FE's board. The WT consist only of a few selected experts, typically from the IT security department (e.g., CISO) and should be complemented by a board level member (e.g., CIO, COO) in order to allow for swift and confidential escalation if needed. The WT acts as a single point of contact between all involved parties and is responsible for the test throughout all phases – from the test design to the operational testing and the identification of improvement measures.

If all hacking attempts in an ongoing test are successfully defended, the WT may also provide guidance to the Red Team (RT, see 3.4) in case assistance (leg-ups, see also footnote 4) is needed. These leg-ups are prepared by the WT well in advance before the attack starts.

Once the test is completed, the WT consults all relevant parties (see section 4.3) in the process of conducting a comprehensive analysis of the results. This includes reviewing all test data, identified vulnerabilities and weaknesses, and developing a Remediation Plan for improving the FE's security posture.

For more information on the roles and responsibilities of a WT, see TIBER-EU White Team Guidance.

3.2 Blue Team (BT)

The FE-internal Blue Team (BT) is responsible for protecting the FE's systems and data from cyberattacks and for fending off attacks from the RT. In principle, the BT comprises all employees of the FE who are not part of the WT. In practice, the BT is, however, usually represented by employees of the units responsible for (cyber) security that is actively involved in the defense of the RT's attacks without their prior knowledge.

The concrete representatives of the BT conveying the learnings from the test can only be established in the closure phase, since it is essential that the BT is unaware of the preparation and conduct of the test. The results and findings will only be meaningful if the FE confines the knowledge of a TIBER-AT test to a strictly limited group of people (i.e. WT, CISO, FE's board), while the remainder of the FE acts without knowledge of the ongoing test.

In the closure phase of the TIBER-AT test, the BT is informed about the test conducted and plays a central role in the post-action analysis. This involves reviewing logs and system data to identify how the attack was able to penetrate the FE's defences. Based on this, the BT produces the Blue Team Report. Together with the RT, the BT subsequently works on enhancing policies, procedures, and technology to prevent similar attacks from occurring in the future (see 3.5).

3.3 Threat Intelligence Provider (TIP)

A TIP is an independent third-party provider that mimics investigation efforts of "real life" threat actors. As such, the TIP is responsible for providing accurate, actionable, Targeted Threat Intelligence (TTI) on the tested FE. This analysis should include relevant information on specific vulnerabilities and weaknesses in the FE's infrastructure and systems that could potentially be exploited. To obtain such knowledge, TIPs conduct appropriate research (e.g., in-depth open-source intelligence, dark web sources). Following the handover from the TIP to the Red Team Provider (RTP), the TIP ideally continues to be accessible, where needed.

As part of the TIBER-AT test, the TIP needs to collaborate closely with the RT to ensure that it builds its attack strategy around the FE's specific vulnerabilities. The TIP provides the RT with up-to-date and relevant TTI to help identify specific attack vectors, social engineering opportunities, and other weaknesses in the target FE's defences.

For more information on TTI reporting, see the TIBER-EU Guidance for Target Threat Intelligence Report.

3.4 Red Team (RT)

The RT is an ethical hacking team external to the FE. It imitates a threat actor who tries to gain access to the FE's systems and data by utilising Tactics, Techniques and Procedures (TTPs) tailored to the FE. Its job is to "stay under the FE's radar" and maintain a high level of secrecy throughout the testing process. The expertise and reliability of the RT is of utmost importance since TIBER-AT tests are conducted on live production systems and must not cause any real harm to the FE's data or IT infrastructure.

Building on the FE-specific information compiled by the TIP, the RT can do its own reconnaissance phase to gather more specific information about the FE. All targeted information should then be used to develop a customised attack plan that takes into account the FE's unique characteristics and vulnerabilities.

During the test, the RT aims at achieving predefined goals ("capturing flags"), such as accessing sensitive data or compromising critical systems. The RT simulates a variety of FE-specific attack scenarios that are defined upfront based on the TTI Report. The utilised TTPs can include any means that a real threat actor would use, such as social engineering (e.g., phishing emails, phone calls), software exploits or malware attacks. After achieving access, RTs are encouraged to gain as many advantages as possible in the FE's systems. If, for any reason, any kind of meaningful access to systems cannot be established, the RT is supposed to request help ("leg-up") from the WT to continue its work.

Throughout the TIBER test, the RT is responsible for documenting and providing details on their actions and findings. The RT documents every step of the exercise, including any reconnaissance activities and initial attack vectors, prioritising vulnerabilities identified and the methods used to exploit them. Documentation also includes a sanitised description of sensitive data that was accessed. Aside from the technical project documentation, the Red Team Test Report also provides context, insights and recommendations to help the FE improve its overall security posture and response readiness.

Additional guidance on RT test planning and reporting can be found in the TIBER-EU Guidance for the Red Team Test Plan and in the TIBER-EU Guidance for the Red Team Test Report.

3.5 Purple Team (PT)

During the closure phase, the PT – consisting of BT and RT members – is established. The PT reviews the test together with the WT (replay workshop, see section 4.3.1) and also discusses potential alternative attack scenarios to better understand how effective the defensive controls were, or would be, against a range of offensive attacks. The integration of different experiences maximises lessons learned that can be obtained from the test.

For more information on establishing purple teaming as a collaborative activity, see TIBER-EU Purple Teaming Best Practices.

3.6 TIBER Test Manager (TTM)

The TTM supports a given FE throughout all phases of its TIBER-AT test and serves as its main contact point. The TTM is involved in all meetings and agreements between the parties of the test. This also applies without restriction to necessary potential ad-hoc communication during the test. The responsibilities of a TTM are:

- Act as the TCT-AT's *contact point to the FE's WT;*
- Monitor the test, *validate its compliance* with the TIBER-AT implementation guide and, based on such validation, provide a respective attestation together with the FMA;
- Contribute to *decisions on deviations from the original plan* (e.g., leg-ups, premature test stops).

The TTM is a member of the TIBER Cyber Team Austria (TCT-AT, see 3.7). He/she is backed up by an alternate in order to ensure that his/her tasks will be fulfilled also in case of absence. For certain TIBER-AT Tests, in particular tests of FEs other than credit institutions, the TTM or his alternate may be from an organisational unit within the FMA (hence outside the TCT-AT) which is not responsible for supervising the tested FE.

3.7 TIBER Cyber Team Austria (TCT-AT)

The centralised TCT-AT acts as the national competence centre for implementing TIBER-EU in Austria. Although the FEs take the lead for their respective TIBER-AT tests, the TCT-AT has a variety of tasks. Its main goals and responsibilities are:

1. To ensure the implementation of TIBER-EU in Austria and continuous updates thereof in alignment with TIBER-EU;
2. To ensure the establishment and distribution of the Generic Threat Landscape (GTL);
3. To identify and invite FEs to participate in TIBER-AT tests and to schedule the conduct of these tests;
4. To accompany TIBER-AT tests and to ensure that they are conducted in accordance with TIBER-AT by hosting the TTM;
5. To act as the point of contact for the FE's WT regarding general questions on TIBER-AT. For a given test, the main point of contact for the FE is the TTM;
6. To liaise closely and on a continuous basis with the ECB's TIBER Knowledge Center (TKC, see 3.8) and other national TCTs;
7. To develop and foster a TIBER community in Austria.

In *Austria,* the *TCT-AT* is *located* at the *Oesterreichische Nationalbank (OeNB)* within a horizontal banking supervision unit that is not involved in the operational supervision of FEs. The TCT-AT works in close cooperation with the *Financial Market Authority (FMA)*. The institutional setup mirrors the implemented structure of financial market supervision in Austria. The FMA is the competent authority for supervising all eligible FEs except for significant institutions (SIs) for which the ECB is the competent authority[1]. In line with their respective national supervisory mandates, the OeNB is in the lead for accompanying all credit institutions in their TIBER-AT tests, while the FMA is operationally more heavily involved in the tests carried out by insurance companies and other types of FEs.

The TCT-AT has a designated contact point at the FMA with a dedicated expertise in cybersecurity with respect to TIBER-AT. The TCT-AT coordinates its work according to the above-mentioned responsibilities with the FMA TIBER-AT contact point.

The TCT-AT liaises with other relevant national stakeholders to complement their national cybersecurity initiatives and to ensure consistency of the GTL with their respective insights.

The TCT-AT can be contacted at tiber@oenb.at.

[1] *Please note that with DORA entering into force in 2025, the ECB will be the competent authority for SIs for all tasks according to DORA including those related to TLPT. However, according to Art. 26 (9) and (10), these tasks can (partly) be delegated to a "single public authority in the financial sector […] at national level", which – in that case - would likely be the FMA in Austria. Still, the concrete assignment of competences for TLPT under DORA has not yet been finally decided.*

3.8 ECB TIBER Knowledge Center (TKC)

The TKC is the centre of expertise for all national TIBER implementations. It comprises representatives of the national TCTs of Member States participating in TIBER-EU. The TKC's objectives are to actively support its members' activities, to further develop the TIBER methodology and to foster exchange and cooperation. No specific test results will be shared with the TKC, although anonymised high-level findings and lessons learned may be shared.

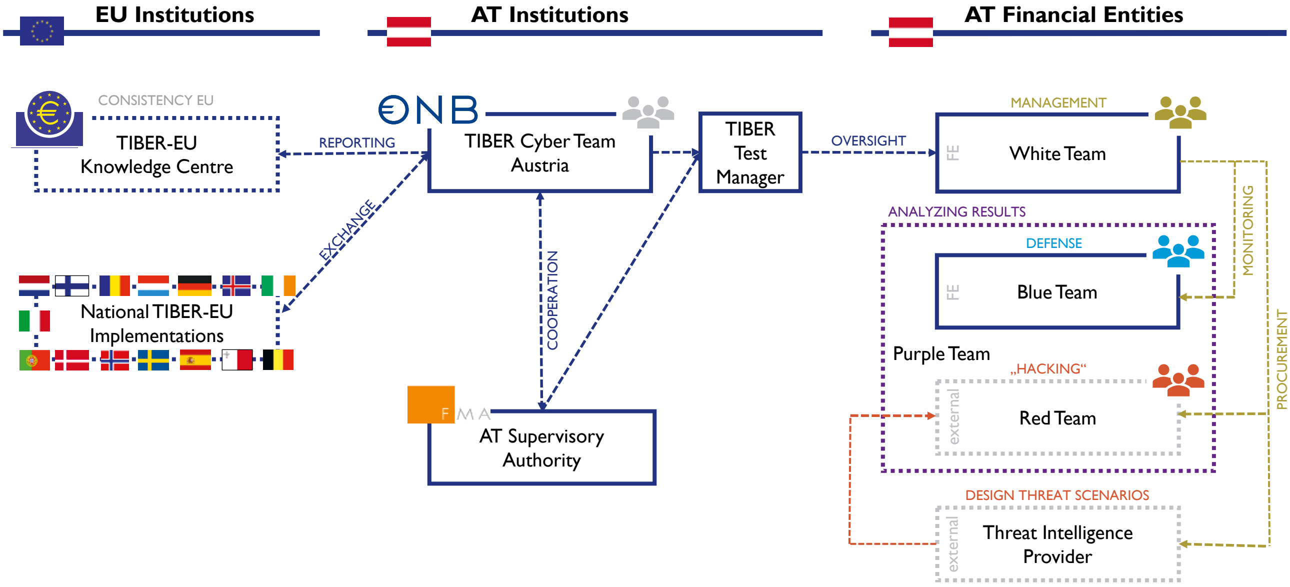
To learn more about the TKC and its activities, see the official webpage of TIBER-EU.

3.9 Interaction of Main Parties of a TIBER-AT test

The following figure shows the main parties of a TIBER-AT test and the major interactions between them.

Figure 2

Interaction of main parties of a TIBER-AT test



Source: OeNB.

4 The phases of a TIBER-AT test

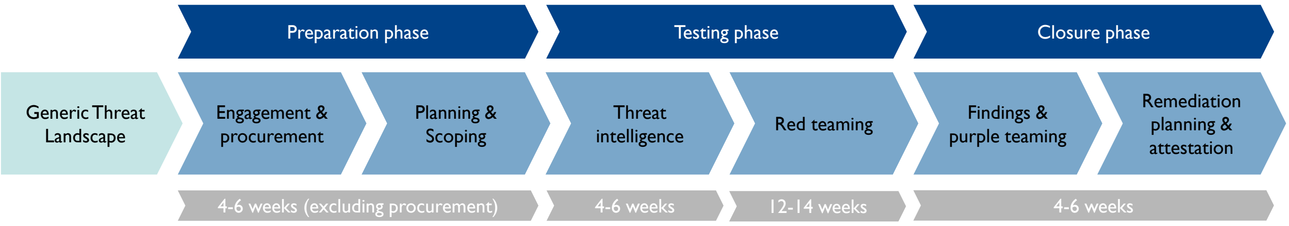
Once the TCT-AT and the FE to be tested have agreed upon undertaking a TIBER-AT test, the predefined testing process will be initiated and the TCT-AT assigns a TTM to the project team of the FE's TIBER test.

A TIBER-AT test consists of three phases: The *preparation phase,* which sets the stage for the whole exercise; the actual *testing phase* consisting of threat intelligence gathering and red teaming; and the final *closure phase,* which focuses on insights and learnings, corresponding remediation measures and formal attestation of compliance with TIBER-AT.

The preparation phase is preceded by the development of a *Generic Threat Landscape (GTL) Report*. This document analyses and details the current potential threats and threat actors relevant to the Austrian financial sector and serves as a starting point for the FE's information gathering and intelligence. The GTL Report is provided to the FEs by TCT-AT.

Figure 3

Generic TIBER-AT process



Source: OeNB.

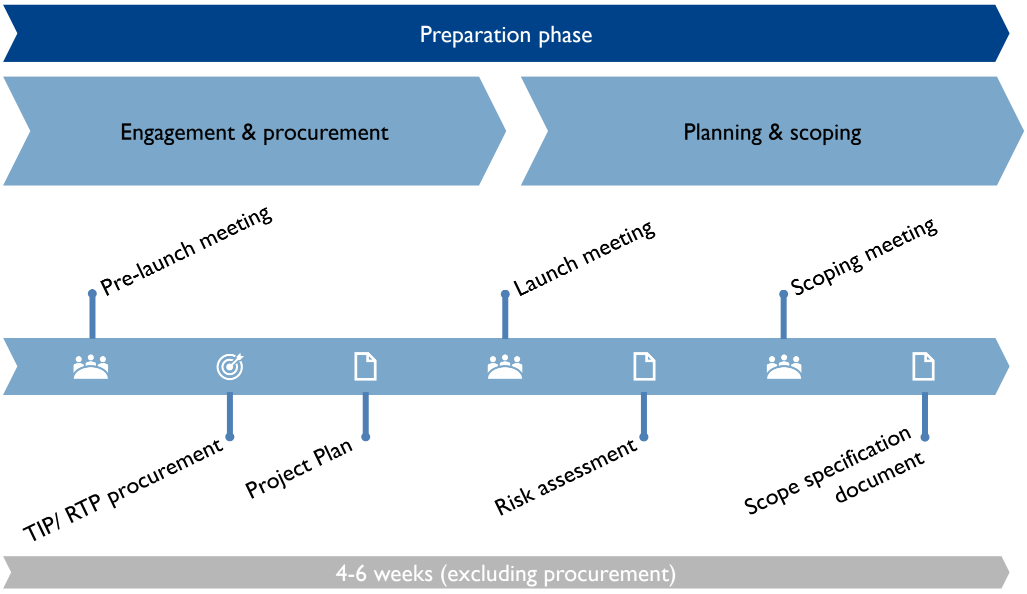
4.1 Preparation phase

This phase starts with the mutual agreement between the TCT-AT and the FE to conduct a TIBER-AT test. It aims at preparing all stakeholders for the subsequent testing procedure and consists of preliminary organisational and planning activities, procurement, the official launch meeting, risk assessment and the definition of the test scope.

At this early stage of the TIBER exercise, the TCT-AT also requests the FE to *establish the WT* and *provide the respective contacts*. The WT subsequently begins with the *project planning* (starting with secrecy and *confidentiality measures* such as the selection of codenames for the project).

Figure 4

TIBER-AT preparation phase



Source: OeNB.

4.1.1 Pre-launch and procurement

The pre-launch meeting marks the *official start* of the TIBER-AT test. In this initial meeting, the TTM outlines the process and the cornerstones of the TIBER-AT test to the WT, in particular:

- The *roles and responsibilities* of the stakeholders;
- The *security protocols* including best practices on secrecy and confidentiality (e.g., secure lines of communication, code names and document transfer channel);
- *Contractual considerations (TIP, RTP)* and specifics on *confidentiality* considerations with respect to *third-party providers* (e.g., document and information sharing);
- Discussion of *cornerstones of the test* such as:
  - Specification and agreement of *codename* for the test,
  - *Critical functions, systems and other potential targets* in/out of scope,
  - Risk assessment and adequate *risk management* including respective controls,
  - *Contingency measures* in case of emergency or involuntary disruptions,
- Allowed and forbidden *Tactics, Techniques and Procedures (TTPs)* e.g., physical red teaming and social engineering; Specifics of *TIBER-AT* and its relation to the TIBER-EU framework.

After the pre-launch meeting the FE begins with the service procurement of TIP and RTP[2]. The minimum requirements are set out in the TIBER-EU Services Procurement Guidelines.

[2] *Ideally, TTI and RT should be provided by separate enterprises. However, if this is not feasible, TTI and RT must not be from the same team.*

4.1.2 Launch meeting

The launch meeting is hosted by the WT with TTM, TIP and RT as participants. The basis of this meeting is the *Project Plan* that is prepared and presented by the WT. The Project Plan must be shared with all stakeholders prior to the launch meeting. It comprises at least:

- *Timeline* and *milestones,* including schedule of meetings and documents to be delivered;
- *Contact points* and *secure lines* of *communication,* including secure document transfer;
- Tested *functions* and underlying systems, *processes* and *technologies;*
- *Risk management* and controls.

The Project Plan as discussed in the launch meeting needs to be approved by the TTM. When the plan has been agreed, the competent *supervisor* is informed by the TCT-AT about the upcoming TIBER-AT test.

4.1.3 Risk assessment

After the launch meeting, the WT conducts a risk assessment to ensure that all the necessary risk management controls, processes, and procedures for a controlled TIBER-AT test are in place and aligned with the FE's existing risk management framework. To reduce the risks associated with testing, sufficient planning and coordination must take place before and during the test.

4.1.4 Scoping and flagging

When defining the test scope and setting the flags regarding the objectives of the test, all CFs must be considered and documented in the scope specification document, including CFs that are fully or partially outsourced to third party service providers. TIBER-EU provides a Scope Specification Template for this purpose. The identified CFs and services need to be aligned with those identified in other FE-specific documents (e.g., recovery plans, resolution plans).

The draft scope specification document is prepared under the remit of the WT in cooperation with the TIP, RT and TTM. It will be discussed and finalised by these stakeholders in their scoping meeting. Before the scoping meeting, the draft scope specification document will be shared with all meeting participants and consulted with the competent supervisor by the TTM to ensure that the scope is a realistic representation of the entity. After the scoping meeting, the scope specification document is approved by the FE's board.

After having been consulted about the draft scope specification document, the competent supervisor will not be re-involved in the TIBER-AT test until the Test Summary Report is shared.

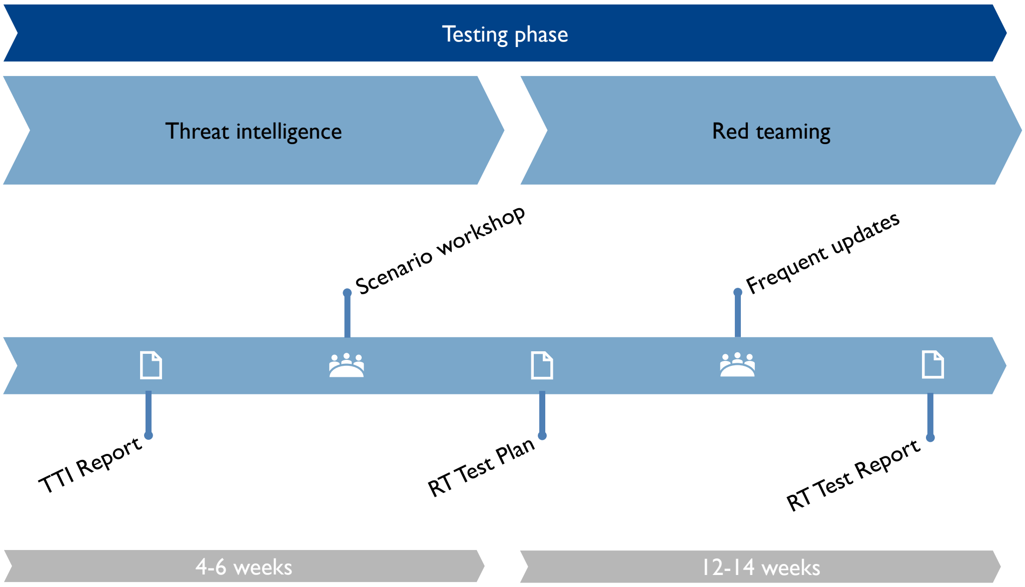
Scoping and flagging complete the preparation phase, which is followed by the testing phase.

4.2 Testing phase

The testing phase comprises a threat intelligence phase and a red teaming phase.

Figure 5

TIBER-AT testing phase



Source: OeNB.

4.2.1 Threat intelligence

With the start of the testing phase, the TIP begins *gathering intelligence* on the tested FE, providing indication of the *progress* and *success* of its *efforts*. Targeted Threat Intelligence (TTI) activities must be conducted in an ethical way, in compliance within applicable laws and without bad intent. Due to the short time frame for gathering actionable intelligence, especially in comparison to actual persistent threat actors, the TTI Report may be *complemented* by *FE-internal information*[3] if deemed useful by the WT.

In due time, the Threat Intelligence Provider (TIP) is expected to provide the *TTI Report,* which gives a comprehensive picture of the FE's weaknesses and potential threat actors. The report builds on information provided by the GTL and should be meaningful, comprehensive and precise enough to be used for the RT's later work. It also includes appropriate realistic attack scenarios based on targeted threat-specific insights from the TIP's investigations.

The TTI Report is presented to the WT, RT and TTM and subsequently discussed and fine-tuned with them in a *scenario workshop,* where concrete actionable attack scenarios are selected for the FE's specific environment and systems. The *final TTI Report* comprises the following details:

[3] *E.g., business and technical overview of each CF-supporting system in scope, current internal threat assessment, examples of recent attacks.*

- *Threat intelligence,* including current significant (types of) threat actors and associated TTPs;
- *Target intelligence,* including information on potential attack surfaces across and throughout the FE.
- *High-level threat scenarios,* based on the threat & target intelligence.

Based on the TTI Report, the WT and the TTM evaluate if the *test scope and the flags need to be updated* in light of recent information. Thereafter, the red teaming phase officially starts. Some overlap between the threat intelligence and the red teaming phase is acceptable, if agreed upon with the WT and the TTM.

For more details about the structure and recommended content of a TTI Report, see the TIBER EU Guidance for Target Threat Intelligence Report.

4.2.2 Red teaming

Once the threat intelligence process is completed, the execution of RT planning and testing commences. This phase needs sufficient time for the RT to conduct a realistic, effective and comprehensive attack on the basis of the TI scenarios. The RT provider further enriches the selected scenarios with its own technical and operational knowledge. Fulfilment of all test objectives and capturing of flags should be achievable for the RT.

For the design of the *RT Test Plan,* the RT aims for deploying a broad range of TTPs during the test, using industry standard methodologies. The RT is also encouraged to spontaneously pivot towards creative, non-standardized TTPs if deemed appropriate and necessary. For further information on the approach and structure of a RT test plan, see the TIBER-EU Guidance for the Red Team Test Plan.

Thereafter, the operational *RT testing* can start. It is required that the WT and the RT agree to monitor its progress on a regular basis (at least weekly) and involve the TTM for consultation. However, potentially critical vulnerabilities and incidents have to be shared without delay.

During its attack runs, the RT performs intelligence-led tests on the target systems along the RT Test Plan, end to end. However, on the basis of insights gained in the meantime adjustments can be made to the RT Test Plan at short notice and leg-ups can be provided, if necessary. Any changes to the original plan need to be approved by the WT and the TTM. The WT may also deliver further information or assist with leg-ups[4] if a test gets stuck. Confidentiality remains particularly important when providing leg-ups and leg-ups must be provided in a covert manner that does not alert the BT.

In any case, the RT needs to thoroughly document each of its steps to allow for later replay activities. The *RT Test Report* is the final output and will be delivered to the WT. It describes the specific TTPs applied during the attacks, the attack results and observations made throughout the process. Lastly, the report contains recommendations on how to improve defence mechanisms and procedures[5].The

[4] *"Leg-ups" are subject to common agreement and understanding (RT, WT and TTM) and can also be adapted on the spot to help unwind a barred test progress. In practice, whatever seems most useful in the current situation will be agreeable, from WT guidance and steering, to provisioning of passwords, to granting direct access to systems, infrastructure and networks.*

[5] *Defence mechanisms and procedures regarding physical and technical security measures, entity-wide policies and procedures, awareness campaigns, specialist training programmes, etc.*

report must be issued within two weeks after RT test completion, so as not to delay the kick-off of the final closure phase and enable swift implementation of measures to remediate potential vulnerabilities.

For more details about the structure and recommended content of a RT Test Report, see the Guidance for the Red Team Test Report.

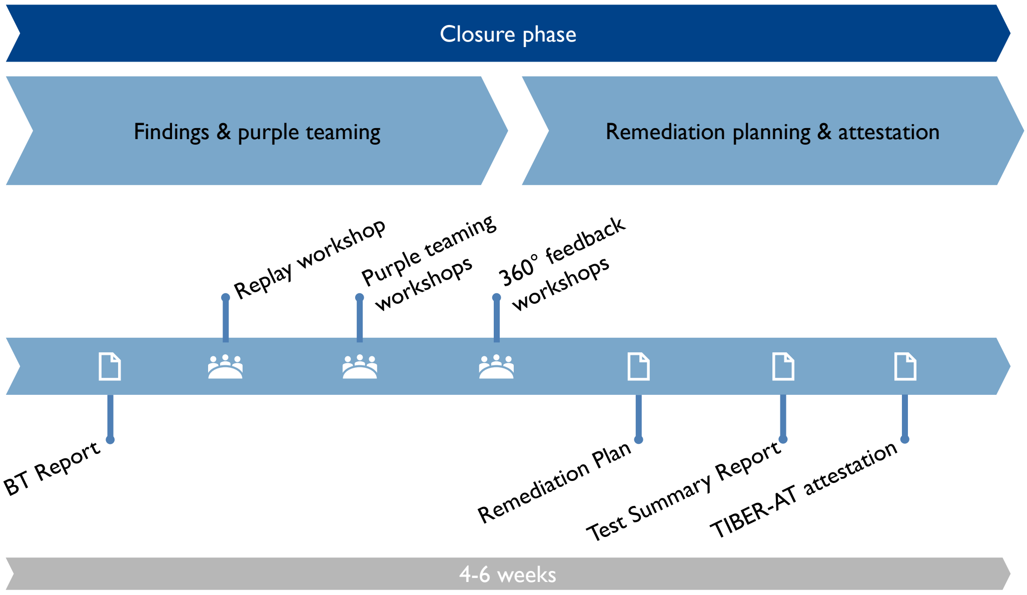
4.3 Closure phase

After the completion of the RT Test Report, the final phase of the TIBER-AT test is aimed at converting the insights from the test into actionable recommendations to the FE. End products in this phase are the BT Report, the Remediation Plan, the Test Summary Report and the final attestation of the TIBER conformity of the test. Please note that the RT Test Report, the BT Report and the Remediation Plan remain at the FE's premises at all times.

The meetings in this phase consist of the purple teaming workshops – focusing on a replay of actions and the discussions of implications – as well as the 360° feedback workshop.

Figure 6

TIBER-AT closure phase



Source: OeNB.

4.3.1 Findings and purple teaming

The closure phase kicks off with the information of the *BT* that a *TIBER-AT test has taken place*. The *RT Test Report* is subsequently *distributed to the BT.* The BT then drafts the *BT Report* based on the RT Test Report. In this report, the BT indicates its reactions and countermeasures for all intrusion attempts of the RT. Both reports, the RT Test Report and the BT Report, are available to the TTM on the FE's premises. After the reports are finalised, the WT invites all involved parties (BT, RT, TTM, optionally TIP) to a series of *purple teaming (PT) workshops.*

First, in the replay of the test *(replay workshop)* the RT and the BT present their actions and counteractions on a step-by-step basis alongside with a discussion on how they experienced the individual steps.

Second, the WT is responsible to conduct *further PT workshops* with all involved parties to discuss the implications of the test and which alternative steps by the BT and the RT could have been taken in reaction to each other. The goal of these PT workshops is to reach a joint understanding how to enhance the cybersecurity and resilience of the FE based on the newly gained insights.

For further supporting material on conducting purple teaming, see the TIBER-EU Purple Teaming Best Practices.

Additionally, the TTM arranges a *360° feedback workshop* to allow all stakeholders to reflect on their TIBER-AT experience and give consideration on how to potentially improve the practical execution of further upcoming tests. Discussions typically centre around:

- Which processes in the test went well/could be improved?
- Which adaptations could have made the test setup smoother?
- Which methodological components of TIBER-AT could need improvements?

As a result, the WT, TIP, RTP and the TCT-AT will obtain feedback. Based thereon, the TCT-AT may update the TIBER-AT implementation guide accordingly. In addition, anonymised feedback regarding the TIBER-EU framework is shared with the TKC on a regular basis.

The execution of any necessary *clean-up tasks* shall also be conducted as part of the closure phase. Clean-up activities may include the removal of deployed beacons, hardware implants, compromised or added files or any other tool that has been deployed by the RT to support their red teaming activities.

4.3.2 Remediation planning and attestation

Based on the discussions in the PT workshops, the FE produces a detailed *Remediation Plan* that lists the *measures* to be taken, the timelines and *milestones* for mitigating individual vulnerabilities, and the necessary *resources* and *responsibilities.*

A high-level summary of the Remediation Plan should be included in the *Test Summary Report* prepared by the WT. In addition, the Test Summary Report summarises in a bird's-eye view the overall test process, results and insights gained. This report is handed over to the TCT-AT.

At the end of the closure phase, the FE's board, TIP and RTP confirm that their parts in the test were conducted in line with TIBER-AT. Thereafter, the TTM validates these confirmations and based on this validation the FMA together with the TTM provide an *attestation* that the test was conducted in accordance with TIBER-AT.

Supplementary information for the Test Summary Report is provided in the TIBER-EU Guidance for the TIBER-EU Test Summary Report. For the test attestation, TIBER-EU offers the TIBER-EU Attestation Template.

After completion of the TIBER-AT test, the TCT-AT informs the competent supervisor that the test has been finalised. Furthermore, the FE shares the Test Summary Report including the high-level summary of the Remediation Plan and the attestation with the competent supervisor.

5 Disclaimer of liability

This document describes the implementation of the TIBER-EU framework in Austria (TIBER-AT) and is intended for informational purposes only. It does not constitute a legal or any other kind of expert assessment and it does not confer rights or impose obligations of any kind on third parties. The FE that conducts a TIBER-AT test remains solely responsible and liable for the execution of the tasks outlined in this guide, including the legal and technical risk assessment (comprising compliance with applicable laws and regulations) of the test and respective safeguards. OeNB, FMA and the ECB cannot be held liable for any damage resulting from the use of this document or from the conduct of TIBER-AT tests.

6 Annex

6.1 RACI Matrix for a TIBER-AT test

The Responsibility, Accountability, Consultation and Information (RACI) Matrix gives a comprehensive overview of the roles and responsibilities of the various stakeholders involved in the course of a TIBER-AT test.

Table A1

RACI Matrix for a TIBER-AT test

	Responsible	Accountable	Consulted	Informed	Relevant Documents	Description
Generic Threat Landscape						
GTL Report	TCT-AT	GTL Provider	Relevant national institutions	Relevant FEs	*Output:* • GTL Report	General overview of the Austrian financial sector threat landscape
Preparation phase						
Engagement & procurement						
Pre-launch meeting	TTM	TTM	WT	FE's board	*Input:* • TIBER-AT Implementation Guide • TIBER-EU White Team Guidance	General agreement on the conduct of a TIBER-AT test between the TCT-AT and the FE concerned
TIP procurement	WT	FE's board	TTM	TIP	*Output:* • Contract with TIP *Input:* • TIBER-EU Framework Services Procurement Guidelines	Procurement process and formal contract with the TIP
RTP procurement	WT	FE's board	TTM	RTP	*Output:* • Contracts with RTP *Input:* • TIBER-EU Framework Services Procurement Guidelines	Procurement process and formal contract with the RTP
Planning & scoping						
Project Plan	WT	WT	TTM, RTP, TIP	-	*Output:* • Project Plan	General timeline and significant milestones of the TIBER-AT test
Launch meeting	WT	FE's board	TTM, RTP, TIP	-	*Output:* • Summary of launch meeting	Agreement on test process, expectations, Project Plan
Risk assessment	WT	FE's board	TTM, RTP, TIP	-	*Output:* • Summary of the risk assessment	Ensuring that the right risk management precautions are in place prior to the test
Scoping	WT	FE's board	TTM, RTP, TIP, Competent Supervisor	-	*Output:* • Scope specification document *Input:* • TIBER-EU Scope Specification Template	Definition of the scope and flags
Testing phase						
Threat intelligence						
TTI Report	TIP	WT	TTM	RTP	*Output:* • TTI Report *Input:* • GTL Report • TIBER-EU Guidance for Target Threat Intelligence Report	Specification of the FE's vulnerabilities and potential attack scenarios (input for RTP)
Scenario workshop	TIP	WT	RTP, TTM	-	*Output:* • Attack scenarios *Input:* • TTI Report	Handover from TIP to RTP

Source: OeNB.

Table A1 continued

RACI Matrix for a TIBER-AT test

	Responsible	Accountable	Consulted	Informed	Relevant Documents	Description
Red teaming						
RT Test Plan	RTP	WT	WT, TTM, TIP	-	*Output:* • RT Test Plan *Input:* • TIBER-EU Guidance for the Red TeamTest Plan • TTI Report	Specification of the TTPs building on the scenarios defined in the TTI Report
Frequent test updates[1]	WT, RTP	WT	TTM	-	-	Discussion on the ongoing test and next steps (e.g., status of flags, necessity for leg-ups[2])
RT Test Report	RTP	WT		TTM, BT	*Output:* • RT Test Report *Input:* • TIBER-EU Guidance for the Red Team Test Report	Report focusing on RT actions and findings Informing of BT only after it has been made aware of the test as part of the closure phase.
Closure phase						
Findings & purple teaming						
BT Report	BT	WT	RTP	TTM	*Output:* • BT Report *Input:* • RT Test Report	Mapping of BT's actions alongside the RT's actions
Replay workshop	WT	WT	RTP, BT, TIP (optional)	TTM	*Input:* • BT Report • RT Report	Replay of the attack and defence actions taken
Purple teaming workshops	WT	WT	RTP, BT, TIP (optional)	TTM	*Output:* • Purple teaming workshop summary *Input:* • TIBER-EU Purple Teaming Best Practices	Discussing alternative routes and course of actions of the BT and RT.
Remediation planning & attestation						
360-degree feedback workshop	TTM	TTM	WT, BT, RTP, TIP	TKC	*Output:* • 360-Degree Feedback Report	Holistic test review focusing on the overall process
Remediation Plan	WT	FE's board	BT, RTP, TIP, TTM		*Output:* • Remediation Plan	Plan to address the identified vulnerabilities (e.g., responsibilities, budgets, timelines)
Test Summary Report	WT	FE's board	RTP, TIP, TTM	Competent supervisor	*Output:* • Test Summary Report *Input:* • All documents elaborated in the course of the test • TIBER-EU Guidance for the TIBER-EU Test Summary Report	High level summary of the overall test process and test results
TIBER-AT attestation	FE's board, FMA, TTM	FE's board	WT, RTP, TIP	Competent supervisor	*Output:* • Signed TIBER-AT attestation *Input* • TIBER-EU Attestation Template	Signed attestation that the test has been conducted in accordance with TIBER-AT

Source: OeNB.

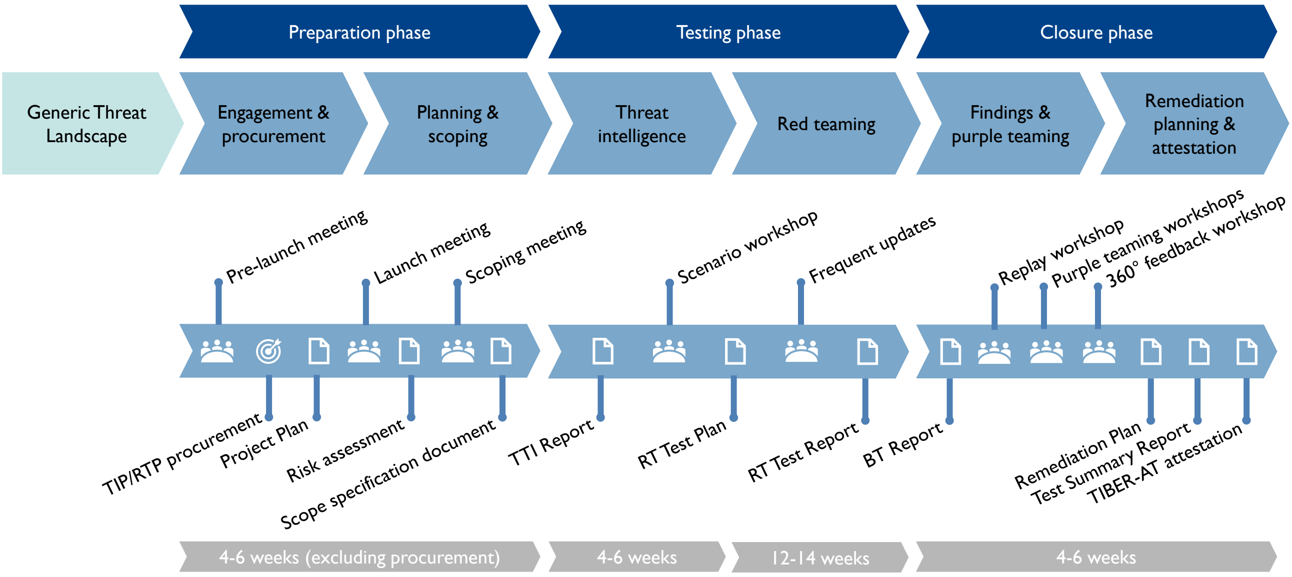
[1] *At least on a weekly basis*

[2] *On ad hoc basis and as appropriate*

6.2 Overview of the full TIBER-AT process

Figure A1

Overview of the full TIBER-AT process



Source: OeNB.

6.3 Glossary

Table A2

Glossary

AT	Austria
BT	Blue Team
CF	Critical Function
CISO	Chief Information Security Officer
DORA	Digital Operational Resilience Act
ECB	European Central Bank
ESCB	European System of Central Banks
EU	European Union
FE	Financial Entity
FMA	Financial Market Authority
GTL	Generic Threat Landscape
ICT	Information and communication technology
OeNB	Oesterreichische Nationalbank
PT	Purple Team
RACI	Responsible, Accountable, Consulted, Informed
RT(P)	Red Team (Provider)
SI	Significant Institution (according to Art. 6 (4) of Council Regulation (EU) No 1024/2013)
TCT	TIBER Cyber Team
TI P	Threat Intelligence Provider
TIBER	Threat Intelligence-Based Ethical Red Teaming
TKC	TIBER Knowledge Center
TLPT	Threat-Led Penetration Testing
TTI	Targeted Threat Intelligence
TTM	TIBER Test Manager
TTP	Tactics, Techniques, and Procedures
WT(L)	White Team (Lead)

Source: OeNB.

6.4 Web sources (Framework, Guidance, Templates)

Table A3

Web sources

Documentation	Content
TIBER-AT Implementation Guide	Guidance on the national implementation and specificities of the TIBER-EU framework applicable for Austria
ECB TIBER Knowledge Center Website	ECB TIBER-EU Website Overview (goal, national implementations, documents)
TIBER-EU framework	How to implement the European framework for Threat Intelligence-based Ethical Red Teaming
TIBER-EU White Team Guidance	The roles and responsibilities of the White Team (Control Team) in a Threat Intelligence-based Ethical Red Teaming test
TIBER-EU Framework Services Procurement Guidelines	Guidance on TIP and RTP requirements, selection principles and exemplary assessment checklists
TIBER-EU Scope Specification Template	Templates for the presentation of the detailed scope of the entity's respective test (scope, flags, key systems and services, etc.)
TIBER-EU Guidance for Target Threat Intelligence Report	Guidance on developing the TTI Report for the entity based on GTL, scope specification and other relevant information
TIBER-EU Guidance for the Red Team Test Plan	Guidance and standardised structure for producing the Red Team Test Plan with focus on testing phase organisation, organisation planning and RT test management
TIBER-EU Guidance for the Red Team Test Report	Guidance on the Red Team Test Report including details of the testing approach taken as well as findings and observations from the testing exercise
TIBER-EU Purple Teaming Best Practices	Main principles and guidance on how purple teaming might be used in the testing and closure phases of a test conducted under the TIBER-EU process
TIBER-EU Guidance for the TIBER-EU Test Summary Report	Guidance for drafting the Test Summary Report with a sanitised, high-level overview of the TIBER-AT test
TIBER-EU Attestation Template	Template confirming the conducted test as a legitimate TIBER-AT test

Source: OeNB.