OESTERREICHISCHE NATIONALBANK
EUROSYSTEM

TIBER-AT Implementation Guide

July 2025

Security through stability

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 (No. 820)

Please collect used paper for recycling.

EU Ecolabel: AT/028/024

EMAS
Verified environmental management
REG.NO. AT- 000311

EU Ecolabel
www.ecolabel.eu

Content

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 on financial entities (FEs). In contrast to most other respective methodologies, TIBER-EU provides for real life tests of operational critical systems without a separate test environment. It is not based on a pass/fail concept; the tests are designed as a learning experience and to bring maximum benefit to the tested FE. Essentially, TIBER-EU is aimed at continuously improving the cyber resilience of the financial sector.

According to the TIBER-EU framework, the tested FE must take all the necessary measures to ensure that no risks arise for the FE or its customers. Consequently, the tests are conducted under strict safety provisions. The costs for a TIBER-EU test are borne by the FEs, requiring them to budget accordingly.

Upon the first publication of the TIBER-EU framework in 2018, the European Central Bank (ECB) established the TIBER-EU Knowledge Centre (TKC) for national authorities. The TKC monitors and supports the consistent national implementation of the TIBER-EU framework. In November 2023, the Oesterreichische Nationalbank (OeNB), together with the Financial Market Authority (FMA), decided to implement the TIBER-EU framework in Austria and published the first TIBER-AT Implementation Guide.

Under the Digital Operational Resilience Act (DORA), Threat-Led Penetration Testing (TLPT) became mandatory for specific FEs as of January 2025 with TIBER-EU as the relevant standard. To be fully compliant with the requirements set out by DORA and the regulatory technical standard (RTS) on TLPT, the TIBER-EU framework was updated in January 2025. With this document, the TIBER-AT Implementation Guide was revised accordingly and published in July 2025. Furthermore, the ECB publishes the first TIBER-EU SSM Guide for TLPT of significant institutions (SIs) within the Single Supervisory Mechanism (SSM)[1].

All requirements of the TIBER-EU framework apply directly and fully to TIBER-AT tests. Consequently, all details on how to conduct a TIBER-AT test are described comprehensively in the TIBER-EU framework. In particular, TIBER-AT includes all mandatory elements of TIBER-EU, is aligned with TIBER-EU SSM and deals with certain national specificities. In addition, TIBER-AT also provides for some elements considered optional under TIBER-EU. Hence, a TLPT conducted in accordance with this TIBER-AT Implementation Guide meets all applicable DORA requirements.

TIBER-AT also allows for voluntary participation. Admission to TIBER-AT tests shall be coordinated with the TIBER Cyber Team Austria (TCT-AT) at the OeNB. For contact details, please refer to section 3.

2 TIBER-AT implementation

2.1 Target audience

TIBER-AT is targeted at Austrian FEs providing core financial services and playing a systemic role in the Austrian financial market. Only FEs that are mature enough from an ICT perspective are required to perform a TLPT. 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.

[1] SIs refer to credit institutions which are classified as significant in accordance with Article 6 (4) SSM Regulation, and hence are under direct supervision from the ECB.

The FMA will identify Austrian FEs listed in Article 2 DORA Enforcement Act (DORA-VG) in line with Article 2 RTS on TLPT as having to perform mandatory TLPT under TIBER-AT. Note that this does not comprise SIs, which are identified by the ECB for mandatory TLPT and hence shall perform their tests based on the TIBER-EU SSM Guide.

The FMA will require each FE it has identified to appoint a Financial Entity Contact Point (FECP) for TLPT to ensure secrecy.[2] The FECP should have sufficient authority along with knowledge of the entity's IT systems and business processes[3]. Once the test begins, the FECP should be included in the control team (CT) according to TIBER-EU. The FECP receives all relevant information on TLPT from the FMA and the TCT-AT. The FE should provide the contact details of the designated FECP to the TCT-AT and inform the TCT-AT without undue delay if the contact details of the FECP change or a new FECP is appointed.

Austrian FEs that are not required to undergo TLPT according to DORA can apply for voluntary tests in accordance with TIBER-AT. Participation in a voluntary TIBER-AT test, however, also requires a certain level of cyber maturity.

2.2 TLPT Authority

The TLPT Authority (TLPTA) designated according to Article 26 DORA is responsible for TLPT-related tasks in the financial sector. While the TIBER-EU framework refers to TIBER Authority in this context, TIBER-AT uses the acronym TLPTA to refer to both terms interchangeably. The FMA is the TLPTA for all Austrian FEs except for SIs, for which the ECB is the TLPTA.

In accordance with Article 6 DORA-VG, the FMA, in its function as TLPTA, will issue an attestation pursuant to Article 26 (7) DORA based on an expert opinion from the OeNB. At the OeNB, expert opinions on TLPT under TIBER-AT are provided by the TCT-AT. With the request for this expert opinion, the FMA delegates certain tasks – assigned to the TLPTA according to the RTS on TLPT – to the TCT-AT (see section 2.3). If the ECB entrusts the TCT-AT with the oversight of an SI's TLPT, a corresponding delegation of tasks from the ECB to the TCT-AT takes place. The final attestation for SIs is always to be issued by the ECB.

2.3 TIBER Cyber Team

A TIBER Cyber Team (TCT) according to TIBER-EU, or a TLPT Cyber Team according to Article 3 RTS on TLPT, is composed of staff involved with TIBER test-related matters, including Test Managers (TMs, see section 2.4). TIBER-AT uses the acronym TCT-AT to refer to both of these terms interchangeably.

In Austria, the centralized TCT-AT is located at the OeNB within an IT supervision division, organized as a separate unit not involved in the operational supervision of FEs. It acts as the national competence center for implementing TIBER-EU in Austria.

The TCT-AT works in close cooperation with the FMA as set out in Article 6 DORA-VG as well as with the ECB. Therefore, the TCT-AT has designated contact points at the FMA and the ECB with expertise in cybersecurity with respect to TIBER. The TCT-AT coordinates its work according to the abovementioned responsibilities with the FMA and the ECB contact points.

[2] In TIBER-EU SSM, the FECP for TLPT is called single point of contact (SPOC).

[3] Usually, these would be individuals holding the role of (or reporting directly or indirectly to) the Chief Information Security Officer, Chief Risk Officer, Chief Technology Officer or Chief Information Officer.

In line with their respective supervisory mandates, the OeNB is in the lead for overseeing tests of credit and other institutions, where the OeNB is substantially involved in their ongoing supervision, while the FMA is operationally more involved in tests carried out by FEs supervised solely by the FMA (see also section 2.4).[4]

In case of multi-jurisdictional tests[5] with participation of an Austrian FE, the responsible TLPTAs shall evaluate, in cooperation with the TCT-AT, their involvement in line with Art. 16 RTS on TLPT.

2.4 Test Manager

For each TIBER-AT test, a dedicated Test Manager (TM) and at least one alternate are assigned from the TCT-AT. The TM alternate(s) are considered equal to the TM for tasks related to the ongoing test. Hence, according to TIBER-AT, the acronym TM subsumes the Test Manager and respective alternate(s). Together, they should have comprehensive cyber security expertise, profound knowledge in the relevant sector of the tested FE as well as proven project management skills.

For TIBER-AT tests of FEs supervised solely by the FMA, such as insurance companies or trading venues,[4] the FMA designates a TM, who is not involved in the operational supervision of the tested FE. The remaining TM is assigned from the TCT-AT. For the duration of the test, the TM assigned by the FMA shall temporarily be considered part of the TCT-AT.

The role of the TM is to make sure that the FE performs the test in accordance with TIBER-AT in a uniform and controlled manner. The TM is particularly responsible for fulfilling the tasks delegated by the TLPTA to the TCT-AT in the context of a specific test (see section 2.2). Upon successful completion of the TIBER-AT test, the TM confirms adherence to the requirements by providing an expert opinion to the TLPTA.

2.5 Test-specific elements

TIBER-AT also provides for some test elements considered optional under TIBER-EU. These include:

- Prior to a TIBER-AT test, the FE receives from the TCT-AT a Generic Threat Landscape (GTL) report provided by the OeNB and the FMA, which highlights the current threat situation for the Austrian financial sector and serves as a starting point for the FE-specific test design.
- Physical red teaming (e.g. planting a device at the FE's premises) is explicitly allowed, provided that all necessary precautions are taken.

Other optional elements according to TIBER-EU may be considered within specific TIBER-AT tests after consultation with the responsible TM.

[4] The FMA is the competent supervisory authority for all FEs listed in Article 2 DORA-VG, which explicitly excludes SIs for which the ECB is the competent authority. The OeNB, however, is substantially involved in the ongoing supervision of FEs listed in Article 2 (1–3, 6, 7) DORA-VG and SIs according to Article 6 (4) SSM Regulation: i.e. all credit institutions, payment and e-money institutions, central security depositors and central counterparties. All other FEs listed in Article 2 (4–5, 8–15) DORA-VG are supervised solely by the FMA (with a few exceptions in targeted areas), in particular insurance companies, pension funds, investment firms, crypto-asset service providers and trading venues.

[5] For further details regarding multi-jurisdictional tests see section 3.7.1 of the TIBER-EU Framework.

3 Contact information

The TCT-AT can be contacted at tct@oenb.at for any questions related to TIBER-AT. The TCT-AT fosters open communication and ensures that any questions or concerns are addressed in a timely and effective manner.

General questions regarding the TIBER-EU framework should be addressed directly to tiber-eu@ecb.europa.eu. The TCT-SSM can be contacted at tct-ssm@ecb.europa.eu for any query related to TLPT of SIs.

4 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 document, including the legal and technical risk assessment (comprising compliance with applicable laws and regulations) of the test and respective safeguards. The OeNB, the 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.

5 Annex

5.1 Glossary

AT	Austria
CT	Control team
DORA	Digital Operational Resilience Act
DORA-VG	DORA Enforcement Act (DORA-Vollzugsgesetz)
ECB	European Central Bank
ESCB	European System of Central Banks
EU	European Union
FE	Financial entity
FECP	Financial Entity Contact Point for TLPT
FMA	Financial Market Authority
GTL	Generic Threat Landscape
ICT	Information and communication technology
OeNB	Oesterreichische Nationalbank
RTS	Regulatory technical standard
SI	Significant institution (according to SSM Regulation)
TCT	TIBER Cyber Team
TIBER	Threat Intelligence-Based Ethical Red Teaming
TKC	TIBER-EU Knowledge Centre (at the ECB)
TLPT	Threat-Led Penetration Testing
TLPTA	Threat-Led Penetration Testing Authority
TM	Test Manager (including their alternate[s])

Source: OeNB.

5.2 Web sources (framework, guidance, templates)

Documentation	Content
OeNB TIBER-AT website	OeNB TIBER-AT website overview including Implementation Guide
ECB TIBER Knowledge Centre 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 SSM Guide	How to implement the TIBER-EU framework for the DORA TLPT of significant institutions
TIBER-EU Initiation Documents Guidance	Guidance on the main project planning aspects of a TIBER test
TIBER-EU Control Team Guidance	The roles and responsibilities of the Control Team in a TIBER test
TIBER-EU Guidance for Service Provider Procurement	Guidance for Threat Intelligence Provider and Red Team Testers requirements, selection principles and exemplary assessment checklists
TIBER-EU Scope Specification Document Guidance	Templates for the presentation of the detailed scope of the FE’s respective test (scope, flags, critical or important systems and services, etc.)
TIBER-EU Targeted Threat Intelligence Report Guidance	Guidance on developing the Targeted Threat Intelligence Report for the FE based on GTL, scope specification and other relevant information
TIBER-EU Red Team Test Plan Guidance	Guidance and standardized structure for producing the Red Team Test Plan with a focus on testing phase organization, risk management, leg-up processes and attack scenarios
TIBER-EU Red Team Test Report Guidance	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 Blue Team Test Report Guidance	Guidance on the Blue Team Test Report including information about the performed red teaming attack actions gathered from the Blue Team
TIBER-EU Purple Teaming Guidance	Main principles and guidance on how purple teaming might be used in the testing and closure phases of a test conducted under the TIBER process
TIBER-EU Test Summary Report Guidance	Guidance for drafting the Test Summary Report with a sanitized, high-level overview of the TIBER test
TIBER-EU Remediation Plan Guidance	Guidance for drafting the Remediation Plan to mitigate the vulnerabilities found during the TIBER test
TIBER-EU Attestation Guidance	Template confirming the conducted test as a legitimate TIBER test

Source: OeNB.