Finantsinspektsioon

TIBER-EE National Implementation Document

This guide describes the implementation of the TIBER-EE framework in Estonia

2026

Finantsinspektsioon

FINANTSINSPEKTSIOON'S
ADVISORY GUIDE

Tallinn

TIBER-EE National Implementation Document

This advisory guide was instated by decision No. 1.1-7/143 of the Management Board of the Financial Supervision Authority on 15.09.2026 pursuant to subsections 57 (1) and (3) of the Financial Supervision Authority Act.

Contents

1. General provisions

1.1. Competence

1.1.1. In accordance with subsection 3 (1) of the Financial Supervision Authority Act (hereinafter *FSAA*), the Financial Supervision Authority (Finantsinspektsioon) conducts state-level financial supervision in order to enhance the stability, reliability, transparency and efficiency of the financial sector, to reduce systemic risks and to promote prevention of the abuse of the financial sector for criminal purposes, with a view to protecting the interests of clients and investors by safeguarding their financial resources, and thereby supporting the stability of the Estonian monetary system.

1.1.2. In accordance with subsection 57 (1) of the FSAA, the Financial Supervision Authority has the right to issue advisory guidelines to explain legislation regulating the activities of the financial sector and to provide guidance to subjects of financial supervision.

1.2. Purpose and area of implementation

1.2.1. This guide (hereinafter the *guide*) is Estonia's national implementation document for the European framework for Threat Intelligence-Based Ethical Red Teaming (hereinafter *TIBER-EU*). The national implementation of the TIBER-EU framework described in this guide is referred to as TIBER-EE. The guide explains the use of TIBER-EE for the purposes of Threat-Led Penetration Testing (hereinafter *TLPT*) in accordance with Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (hereinafter *DORA*).

1.2.2. The purpose of DORA is to strengthen the digital operational resilience of the financial sector by establishing harmonised requirements, including requirements relating to ICT risk management, the management and reporting of ICT-related incidents, digital operational resilience testing, and the management of risks related to third-party ICT service providers. DORA applies to the financial entities referred to in Article 2 of the Regulation, subject to the exemptions set out in that Article. Pursuant to Article 26 of DORA, financial entities identified for this purpose by the competent authority are required to conduct TLPT periodically.

1.2.3. In Estonia, the Financial Supervision Authority is the competent authority under DORA for the financial entities falling within its supervisory remit. In that capacity, and as the TLPT authority, the Financial Supervision Authority applies TIBER-EE as the national implementation of the TIBER-EU framework for the

conduct of TLPT in respect of financial entities falling within the Financial Supervision Authority's TLPT remit.

1.2.4. TIBER stands for Threat Intelligence-Based Ethical Red Teaming. It is a framework for conducting controlled, intelligence-led testing of critical or important functions and supporting systems in production environments, with the objective of strengthening the cyber resilience and operational preparedness of the tested entity.

1.2.5. TIBER-EE should be understood as a resilience-enhancing and learning-oriented framework. It is not intended as a pass-or-fail exercise, but as a structured and controlled means of helping financial entities identify strengths, weaknesses and improvement needs in their protection, detection and response capabilities, while ensuring that testing is carried out safely and responsibly.

1.2.6. This guide should be read together with the TIBER-EU framework and related guidance issued by the European Central Bank (hereinafter *ECB*)[1], as well as the Regulatory Technical Standards (hereinafter *RTS*) on TLPT adopted under DORA (Commission Delegated Regulation (EU) 2025/1190)[2].

1.2.7. The Financial Supervision Authority may provide or identify additional references, templates or contact points relevant to the application of TIBER-EE in Estonia.

1.2.8. All mandatory requirements of the TIBER-EU framework apply directly to TIBER-EE tests. This guide does not restate the full TIBER-EU methodology. Rather, it sets out the national governance model and specificities applicable in Estonia. TIBER-EE constitutes Estonia's national implementation of the TIBER-EU framework and, within the scope of this guide, provides the methodological framework for conducting TLPT under DORA.

1.2.9. In accordance with the RTS, financial entities required to perform TLPT may refer to and use the TIBER-EU framework or a national implementation document, provided that such framework or document is consistent with Articles 26 and 27 of DORA and the requirements set out in the RTS.

---

[1] https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html

[2] https://eur-lex.europa.eu/eli/reg_del/2025/1190/oj/eng

1.2.10. This guide is intended for

- Estonian financial entities identified by the Financial Supervision Authority as subject to TLPT under DORA and in respect of which a corresponding supervisory decision has been issued;
- other Estonian financial entities that wish to conduct a TIBER-EE test on a voluntary basis; and
- third-party service providers and other parties participating in TIBER-EE tests.

1.2.11. For financial entities identified by the Financial Supervision Authority as subject to TLPT under DORA and in respect of which a corresponding supervisory decision has been issued, this TIBER-EE guide constitutes the national framework for the conduct of such testing. Other financial entities may make use of TIBER-EE on a voluntary basis, subject to prior agreement with the Financial Supervision Authority.

1.2.12. TIBER-EE applies within the Estonian financial sector to the extent set out in this guide, taking into account the specific arrangements set out in section 4.5. Other sectors may apply the TIBER-EU framework on a voluntary basis; however, such tests fall outside the scope of this guide and outside the TIBER-EE governance arrangements administered by the Financial Supervision Authority.

1.3. Legal disclaimer

1.3.1. This guide describes the implementation of the TIBER-EU framework in Estonia and is intended as an advisory guide. The guide does not constitute legal advice, does not replace applicable legislation or binding regulatory requirements, and should be read together with the applicable legal and regulatory framework.

1.3.2. In applying this guide, the “comply or explain” principle should be observed, according to which a financial entity must, where necessary, be able to explain why it does not apply a particular provision of the guide or applies it only partially. This principle does not relieve the financial entity of its obligation to comply with mandatory requirements arising from the legislation applicable to the test or from the TIBER-EU framework. A deviation from the provisions of the guide may affect the issuance of an attestation by the Financial Supervision Authority if, as a result of the deviation, the test has not been conducted in accordance with the requirements applicable to it.

1.3.3. The financial entity conducting a TIBER-EE test remains responsible for the execution of the tasks outlined in this guide, including legal and technical risk assessments of the test, the implementation of appropriate safeguards, and compliance with applicable laws and regulations.

1.3.4. The Financial Supervision Authority and the ECB cannot be held liable for any damage resulting from the use of this guide or from the conduct of a TIBER-EE test.

1.4. Contact

1.4.1. Enquiries regarding TIBER-EE and this guide may be addressed to the Financial Supervision Authority at: TLPT@fi.ee.

1.4.2. Enquiries regarding an ongoing test should be addressed to the assigned Test Manager or Alternate Test Manager.

1.4.3. Each financial entity conducting or preparing a TIBER-EE test must designate an appropriate point of contact for communication with the Financial Supervision Authority's TLPT Cyber Team (TCT-EE), ensuring confidentiality and coordination. The designated point of contact must have sufficient authority and an appropriate understanding of the entity's critical functions, systems and internal decision-making arrangements.

2. Governance in Estonia

2.1. Official statement of adoption

2.1.1. The adoption of the TIBER-EU framework for the Estonian financial sector was instated by decision no 1.1-7/67 of the Management Board of the Financial Supervision Authority on 5 May 2025.

2.2. Designated authority

2.2.1. In accordance with Article 26(9) of DORA, each Member State may designate a single competent authority responsible for TLPT in the financial sector. The TIBER-EU framework refers to this function as the TIBER authority, whereas the RTS on TLPT use the term TLPT authority. For the purposes of this guide, these terms are considered equivalent.

2.2.2. The Financial Supervision Authority is an independent financial supervision and resolution authority operating on behalf of the Republic of Estonia. The FSAA authorises the Financial Supervision Authority to perform tasks arising from DORA and to cooperate in cybersecurity with national and Union authorities. It also provides the basis for cooperation with the Information System Authority (hereinafter *RIA*) in matters related to digital operational resilience and TLPT.

2.2.3. For the purposes of TIBER-EE in Estonia, the Financial Supervision Authority acts as the TLPT authority in respect of Estonian financial entities falling within its TLPT remit. For mandatory TLPTs of Significant Institutions (hereinafter SIs) directly supervised by the ECB, the ECB acts as the TLPT authority.

2.3. Role of the designated authority

2.3.1. In its role as TLPT authority, the Financial Supervision Authority oversees the national implementation of TIBER-EE. In particular, it:

- establishes and maintains the TCT-EE;
- coordinates the initiation, planning, and supervisory oversight of TIBER-EE tests;
- reviews and validates key test artefacts and deliverables; and
- issues an attestation upon completion of a test in accordance with the applicable requirements.

2.3.2. The involvement of the Financial Supervision Authority is intended to support the consistency, safety and quality of testing under TIBER-EE and to ensure alignment with DORA, the RTS on TLPT and the TIBER-EU framework.

2.3.3. In the context of TLPT, the role of the Financial Supervision Authority is limited to supervisory oversight and quality assurance. The Financial Supervision Authority does not participate in the operational execution of the test. The financial entity under test, together with its appointed service providers, is responsible for conducting the test.

2.3.4. Where a test falling within the Financial Supervision Authority's TLPT remit has been conducted in accordance with the applicable DORA, RTS on TLPT, TIBER-EU and TIBER-EE requirements, the Financial Supervision Authority issues an attestation confirming that the test was conducted under the relevant framework and national governance arrangements.

2.3.5. Where required by the applicable framework and having regard to the nature of the test, the Financial Supervision Authority cooperates with the ECB, other TLPT authorities and other relevant authorities. Cross-border, joint and pooled TLPTs are coordinated in accordance with, inter alia, the RTS on TLPT.

2.3.6. The Financial Supervision Authority may update this guide as necessary to reflect developments in TIBER-EU, DORA, regulatory technical standards, supervisory practice or national implementation needs.

3. TLPT Cyber Team (TCT-EE)

3.1.1. A dedicated Estonian TLPT Cyber Team (TCT-EE) has been established within the Financial Supervision Authority for the purposes of TIBER-EE and TLPT under DORA. Under the TIBER-EU framework, TCT stands for TIBER Cyber Team, while the RTS on TLPT uses the term TLPT Cyber Team. For the purposes of this guide, these terms are considered equivalent.

3.1.2. The TCT-EE operates within the Financial Sector IT Supervision Department of the Financial Supervision Authority and is responsible for the day-to-day management and operationalisation of the TIBER-EE programme.

3.1.3. The TCT-EE performs the coordination tasks necessary to support and ensure that TLPT is conducted in accordance with DORA, the RTS on TLPT, the TIBER-EU framework and this guide.

3.1.4. The TCT-EE consists of Test Managers and Alternate Test Managers, whose roles and responsibilities are assigned on a test-by-test basis.

3.1.5. Where necessary, the Financial Supervision Authority may draw on external expertise, including expertise from RIA, subject to appropriate safeguards for confidentiality, independence and the management of conflicts of interest.

4. National specifics

4.1. Generic Threat Landscape

4.1.1. The Financial Supervision Authority may make available a Generic Threat Landscape (GTL) document for the Estonian financial sector.

4.1.2. The GTL provides a high-level overview of relevant cyber threats, threat actors, tactics, techniques and procedures, and other developments in the cyber threat environment that may be relevant for TIBER-EE tests.

4.1.3. The GTL is a supporting input to the preparation of TIBER-EE tests. The use of a GTL does not replace the requirement for test-specific threat intelligence, which remains an integral part of each TIBER-EE test in accordance with the TIBER-EU framework.

4.2.Confidentiality and information security

4.2.1. All information exchanged in the context of a TIBER-EE test should be handled in accordance with an appropriate information classification scheme agreed for the test, such as the Traffic Light Protocol (TLP) or another scheme providing an equivalent level of information protection.

4.2.2. Secure communication channels must be used throughout the test. The specific communication arrangements, including encryption and access controls, should be agreed during the preparatory phase of the test.

4.2.3. All TIBER-EE activities must be conducted in accordance with applicable law, including requirements relating to data protection, confidentiality and criminal law. Ethical and safety requirements must be followed in accordance with the TIBER-EU framework.

4.2.4. All test data, reports and related documentation should be treated as restricted information and shared only on a need-to-know basis, in order to preserve the integrity, secrecy and safe conduct of the test.

4.2.5. The financial entity under test must ensure that external service providers are also subject to appropriate confidentiality, independence and conflict-of-interest requirements.

4.3. Sharing of information and results

4.3.1. The sharing of information relating to a TIBER-EE test is subject to applicable law, supervisory confidentiality obligations and any relevant national or international cooperation arrangements.

4.3.2. Test-related information is not shared with other national or foreign authorities, including other supervisors, unless there is a legal basis for such sharing or the tested entity has provided its written consent.

4.3.3. Subject to applicable legal and cooperation arrangements, certain high-level artefacts may be shared with other TCTs for recognition, coordination or consistency purposes.

4.3.4. Without prejudice to applicable confidentiality requirements, the Financial Supervision Authority may encourage the sharing of sufficiently generalised and anonymised lessons learned where information enabling the tested entity to be identified directly or indirectly has been removed from the materials, and the sharing supports broader resilience in the financial sector and does not compromise the confidentiality or safety of the tested entity.

4.4. Cooperation with the Information System Authority

4.4.1. Where necessary, the Financial Supervision Authority cooperates with RIA on matters related to TIBER-EE, TLPT and digital operational resilience, including by drawing on threat intelligence and technical expertise.

4.4.2. Cooperation with RIA is based on clause 4 of subsection (1) of § 47^{11} of the FSAA.

4.4.3. Cooperation may include, as appropriate, the exchange of relevant information, the use of technical or subject-matter expertise, and cooperation in matters related to the preparation of a GTL.

4.4.4. Any cooperation shall be carried out in accordance with the applicable legal basis, confidentiality requirements and the specific circumstances of the test.

4.4.5. Cooperation with RIA does not alter the allocation of responsibilities of the TLPT authorities set out in section 2.2.

4.5. Significant Institutions under the European Central Bank

4.5.1. For mandatory TLPTs of SIs directly supervised by the ECB, the ECB acts as the TLPT authority in accordance with the applicable Union framework.

4.5.2. The ECB TIBER-EU SSM Implementation Guide applies to mandatory TLPTs of SIs identified by the ECB as subject to TLPT under DORA[3].

4.5.3. Where the ECB assigns an SI's TLPT to TCT-EE for oversight, TCT-EE performs the assigned tasks in accordance with the ECB TIBER-EU SSM Implementation Guide.

4.5.4. The final attestation for SIs is always issued by the ECB.

5. Application

This guide will enter into force on 15.09.2026.

[3] https://www.bankingsupervision.europa.eu/ecb/pub/pdf/ssm.supervisory_guide202511.en.pdf

Annex 1. Abbreviations

Abbreviation	Meaning
DORA	The Digital Operational Resilience Act
ECB	European Central Bank
FSAA	Financial Supervision Authority Act
GTL	Generic Threat Landscape
RIA	Information System Authority
RTS	Regulatory Technical Standards
SI	Significant Institution
TCT-EE	Estonian TLPT Cyber Team
TIBER-EE	National implementation of TIBER-EU in Estonia
TIBER-EU	European framework for Threat Intelligence-Based Ethical Red Teaming
TLPT	Threat-Led Penetration Testing
TLP	Traffic Light Protocol