FMA
Finanzmarktaufsicht
Liechtenstein

FMA Communication 2025/3 – Adoption of TIBER-EU LI (implementation document)

Communication on implementation of the TIBER-EU framework in Liechtenstein (TIBER-EU LI)

Reference:	FMA-M 2025/3
Addressees:	All financial intermediaries falling within the scope of Article 2 of Regulation (EU) 2022/2554 (DORA)
Enactment:	7 October 2025
Entry into force:	15 October 2025
Last amendment:	-
Legal basis:	Article 26 of Regulation (EU) 2022/2554 (DORA)

Landstrasse 109 • Postfach 279 • 9490 Vaduz • Liechtenstein
Telefon +423 236 73 73 • www.fma-li.li • info@fma-li.li

FMA

1. Introduction

Testing is an important component of Regulation (EU) 2022/2554, the Digital Operational Resilience Act (DORA), to ensure digital operational resilience. For the purpose of assessing preparedness for handling ICT-related incidents, of identifying weaknesses, deficiencies and gaps in digital operational resilience, and of promptly implementing corrective measures, financial intermediaries are required to establish a sound and comprehensive digital operational resilience testing programme as an integral part of the ICT risk-management framework. For a subset of financial intermediaries within the scope of DORA, advanced testing of ICT tools, systems and processes based on threat-led penetration testing (TLPT) is also provided for in accordance with Article 26 DORA.

TLPT involves performing a series of realistic attack scenarios on critical live production systems to reveal vulnerabilities and strengthen defences. While the DORA requirements provide the basic framework, corresponding guidance should go further and define specific requirements. For this purpose, the TIBER (Threat Intelligence-Based Ethical Red Teaming) framework is being adopted in Liechtenstein. The implementation of TIBER-EU LI aims to test and strengthen the cyberdefence capabilities of financial intermediaries when conducting these tests in line with a proven standard.

2. What is TIBER-EU?

TIBER-EU is a common European framework developed and published by the European Central Bank (ECB) in 2018 that enables controlled, bespoke, and threat intelligence-based red team testing of financial institutions' critical live production systems. TIBER-EU was created as a tool to test and improve key elements of the cyber resilience of participating financial intermediaries, with a focus on the learning effect of the tests.

The TIBER-EU framework has the following core objectives:

- enhance the cyber resilience of financial intermediaries and of the financial sector;
- standardise and harmonise how threat-led red team tests are performed in the EU;
- provide guidance to authorities on how they might implement and manage this form of testing at a national or European level;
- help financial intermediaries and supervisory authorities to fulfil the requirements to perform TLPT as per established regulations through the use of TIBER-EU;
- the TIBER-EU framework may be used as a handbook or set of detailed guidelines on how to complete DORA TLPT in a qualitative, controlled and safe manner – one which is consistent and uniform throughout the EU;
- support cross-border, cross-framework thread-led red team testing for multi-jurisdictional financial intermediaries;
- foster mutual recognition of tests across the EU jurisdictions, by relying on test results and collaborating on joint tests, thereby reducing the regulatory burden on financial intermediaries and supervisory authorities;
- catalyse information sharing and the joint analysis of test results.

3. Adoption of TIBER-EU in Liechtenstein

3.1 About TIBER-EU LI

Pursuant to Article 4 of the EEA DORA Implementation Act (EEA-DORA-DG), the Financial Market Authority (FMA) Liechtenstein is the competent authority for Liechtenstein as referred to in Article 46 DORA. The TIBER-EU framework has been adopted for the financial sector in Liechtenstein and is used to implement the requirements for TLPT in accordance with Article 26 DORA.

Depending on the resources available to the FMA and taking into account an appropriate lead time, tests may be carried out on a voluntary basis in accordance with the relevant standards within the framework of TIBER-EU LI at the request of financial intermediaries, provided that such a test appears necessary or appropriate to the FMA, taking into consideration systemic importance as well as the scale and complexity of the ICT architecture and/or the ICT risk. The decision on whether a test is to be conducted rests with the FMA.

3.2 TIBER-EU LI target sectors

The adoption of the TIBER-EU LI framework is aimed at financial intermediaries within the scope of DORA in accordance with Article 2(1) DORA and is therefore limited to the financial sector.

The TIBER-EU LI framework is particularly relevant for financial intermediaries that are required to perform TLPT based on the following factors as set out in Article 26(8) DORA:

- impact-related factors, in particular the extent to which the services provided and activities undertaken by the financial entity impact the financial sector;
- possible financial stability concerns, including the systemic character of the financial entity at Union or national level, as applicable;
- specific ICT risk profile, level of ICT maturity of the financial entity or technology features involved.

Furthermore, the TIBER-EU LI framework is aimed at financial intermediaries that wish to perform TIBER tests on a voluntary basis in accordance with the relevant standards. In this regard, the FMA refers to the explanations in section 3.1.

Financial intermediaries that are required to perform TLPT are expressly informed of this obligation by the FMA.

4. Role and responsibilities of the FMA

4.1 TIBER and TLPT Cyber Team

The FMA acts as the competent authority for accompanying TLPT and TIBER tests as part of its legal mandate to implement the requirements of DORA. Within the FMA, the *ICT Supervision and Cybersecurity* Unit forms the TIBER and TLPT Cyber Team (TCT).

The FMA's TCT is responsible for the following tasks:

- maintaining and further developing the TIBER-EU LI implementation document;
- enabling and accompanying TIBER tests and TLPT;
- acting as a point of contact for enquiries regarding TLPT and the national implementation of TIBER.

The aim is to achieve pan-European convergence by liaising with other TCTs and participating in activities of the ECB's TIBER-EU Knowledge Centre (TKC), training, and best practices sharing.

The TCT is functionally separate from the supervisory activities of the FMA.

4.2 Contact details

For any questions regarding TIBER-EU LI, the FMA's TCT can be contacted at the following email address: TCT@fma-li.li

5. Reference to TIBER-EU

Within the framework of TIBER-EU LI, the documents of the TIBER-EU framework are applied in their current version without national adaptation. The following website provides a complete overview of all documents relevant to TIBER-EU LI:

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

6. Final provisions and entry into force

This Communication was approved by the Executive Board of the FMA on 7 October 2025 and enters into force on 15 October 2025.