

FMA-Mitteilung 2025/3 – Übernahme TIBER-EU LI (Umsetzungsdokument)

Mitteilung betreffend die Umsetzung des TIBER-EU Rahmenwerks in Liechtenstein (TIBER-EU LI).

Referenz:	FMA-M 2025/3
Adressaten:	Alle Finanzintermediäre, welche in den Geltungsbereich von Art. 2 der Verordnung (EU) Nr. 2022/2554 (DORA) fallen.
Erlass:	7. Oktober 2025
Inkraftsetzung:	15. Oktober 2025
Letzte Änderung:	-
Rechtliche Grundlagen:	Art. 26 der Verordnung (EU) Nr. 2022/2554 (DORA)

1. Einleitung

Ein wichtiger Baustein der Verordnung (EU) 2022/2554, dem Digital Operational Resilience Act (DORA) zur Sicherstellung der digitalen operationalen Resilienz ist das Testen derselben. Um die Vorbereitung auf die Handhabung IKT-bezogener Vorfälle zu bewerten, Schwächen, Mängel und Lücken in Bezug auf die digitale operationale Resilienz zu erkennen und Korrekturmassnahmen umgehend umzusetzen, haben Finanzintermediäre ein solides und umfassendes Programm für das Testen der digitalen operationalen Resilienz als integralen Bestandteil des IKT-Risikomanagementrahmens einzurichten. Für einen Teilbereich der Finanzintermediäre im Geltungsbereich von DORA sind gemäss Art. 26 DORA zudem erweiterte Tests von IKT-Tools, -Systemen und -Prozessen auf Basis von bedrohungsorientierten Penetrationstests (Threat-Led Penetration Testing [TLPT]) vorgesehen.

Bei den TLPT geht es darum, eine Reihe von realistischen Angriffsszenarien auf die kritischen Live-Produktionssysteme durchzuführen, um Schwachstellen aufzudecken und Abwehrmassnahmen zu stärken. Während die DORA-Anforderungen den grundsätzlichen Rahmen vorgeben, sollten entsprechende Anleitungen darüber hinausgehen und spezifische Anforderungen definieren. Zu diesem Zweck wird in Liechtenstein das TIBER (Threat Intelligence-Based Ethical Red teaming) Rahmenwerk übernommen. Die Umsetzung von TIBER-EU LI zielt darauf ab, die Cyberabwehrfähigkeiten von Finanzintermediären bei der Durchführung dieser Tests anhand eines erprobten Standards zu prüfen und zu stärken.

2. Was ist TIBER-EU?

TIBER-EU ist ein gemeinsamer europäischer Rahmen, entwickelt und publiziert von der Europäischen Zentralbank (EZB) im Jahr 2018, der einen kontrollierten, massgeschneiderten und auf Bedrohungsdaten basierten Red-Team-Test der kritischen Live-Produktionssysteme von Finanzunternehmen ermöglicht. TIBER-EU wurde als Instrument für die Prüfung und Verbesserung von Schlüsselementen der Cyber-Resilienz der teilnehmenden Finanzintermediäre geschaffen, wobei der Schwerpunkt auf den durch die Tests gebotenen Lernmöglichkeiten liegt.

Das TIBER-EU Rahmenwerk verfolgt folgende Kernziele:

- die Cyber-Resilienz von Finanzintermediären und des Finanzsektors verbessern;
- die Durchführung von bedrohungsorientierten Red-Team-Tests in der EU zu standardisieren und zu harmonisieren;
- den Aufsichtsbehörden Leitlinien zur Verfügung stellen, wie sie diese Art von Tests auf nationaler oder europäischer Ebene durchführen und verwalten können;
- Unterstützung von Finanzintermediären und Aufsichtsbehörden bei der Erfüllung der Anforderungen zur Durchführung von TLPT gemäss den geltenden Vorschriften durch den Einsatz von TIBER-EU;
- das TIBER-EU-Rahmenwerk kann als Handbuch oder als detaillierte Leitlinie für die qualitative, kontrollierte und sichere Durchführung von DORA-TLPT verwendet werden – und zwar in einer Weise, die in der gesamten EU einheitlich und konsistent ist;
- Unterstützung grenzüberschreitender, rahmenübergreifender, bedrohungsorientierter Red-Team-Tests für Finanzintermediäre, die grenzüberschreitend tätig sind;
- die gegenseitige Anerkennung von Tests in den EU-Mitgliedstaaten fördern, indem auf Testergebnisse zurückgegriffen und bei gemeinsamen Tests zusammengearbeitet wird, wodurch der Verwaltungsaufwand für Finanzintermediäre und Aufsichtsbehörden verringert wird;
- den Informationsaustausch und die gemeinsame Analyse von Testergebnissen fördern.

3. Übernahme von TIBER-EU in Liechtenstein

3.1 Über TIBER-EU LI

Die Finanzmarktaufsicht (FMA) Liechtenstein ist gemäss Art. 4 EWR-DORA-Durchführungsgesetz (EWR-DORA-DG) die für Liechtenstein zuständige Behörde nach Art. 46 DORA. Das TIBER-EU Rahmenwerk wurde für den Finanzsektor in Liechtenstein übernommen und wird für die Umsetzung der Anforderungen an die TLPT gemäss Art. 26 DORA herangezogen.

Abhängig von zur Verfügung stehenden Ressourcen auf Seiten der FMA und unter Berücksichtigung einer entsprechenden zeitlichen Vorlaufzeit, können im Rahmen von TIBER-EU LI auf Wunsch von Finanzintermediären Tests auf freiwilliger Basis nach den entsprechenden Standards durchgeführt werden, sofern ein entsprechender Test unter Betrachtung der systemischen Relevanz sowie des Umfangs, der Komplexität der IKT-Architektur und/oder des IKT-Risikos erforderlich oder der FMA sinnvoll erscheint. Die Entscheidung hinsichtlich der Durchführung des Tests obliegt der FMA.

3.2 Zielsektoren im Rahmen von TIBER-EU LI

Die Übernahme des TIBER-EU LI Rahmenwerks richtet sich an Finanzintermediäre im Geltungsbereich von DORA gemäss Art. 2 Abs. 1 DORA und ist damit auf den Finanzsektor beschränkt.

Konkrete Relevanz hat das TIBER-EU LI Rahmenwerk für Finanzintermediäre, welche aufgrund folgender Faktoren gemäss Art. 26 Abs. 8 DORA verpflichtet sind, einen TLPT durchzuführen:

- wirkungsbezogenen Faktoren, darunter insbesondere inwieweit sich die vom Finanzunternehmen erbrachten Dienstleistungen und ausgeführten Tätigkeiten auf den Finanzsektor auswirken;
- etwaigen Bedenken hinsichtlich der Finanzstabilität, einschliesslich des systemischen Charakters des Finanzunternehmens auf Unionsebene oder auf nationaler Ebene, je nach Sachlage;
- dem spezifischen IKT-Risikoprofil, dem IKT-Reifegrad des Finanzunternehmens oder einschlägigen technologischen Merkmalen.

Weiters richtet sich das TIBER-EU LI Rahmenwerk an Finanzintermediäre, welche TIBER-Tests auf freiwilliger Basis nach den entsprechenden Standards durchführen möchten. Diesbezüglich verweist die FMA auf die Ausführungen in 3.1.

Finanzintermediäre, welche dazu verpflichtet sind, einen TLPT durchzuführen, werden von der FMA explizit über die Verpflichtung informiert.

4. Rolle und Verantwortlichkeiten der FMA

4.1 TIBER bzw. TLPT-Cyberteam

Die FMA fungiert als zuständige Behörde zur Begleitung von TLPT bzw. TIBER Tests im Rahmen des gesetzlichen Auftrags zur Umsetzung der Anforderungen von DORA. Innerhalb der FMA bildet die Fachstelle *IKT-Aufsicht und Cybersicherheit* das TIBER bzw. TLPT-Cyberteam (TCT).

Das TCT der FMA übernimmt dabei folgende Aufgaben:

- Pflege und Weiterentwicklung des TIBER-EU LI Umsetzungsdokument;
- Ermöglichung und Begleitung von TIBER-Tests bzw. TLPT;

- Funktion als Ansprechpartner für Anfragen zu TLPT sowie der nationalen Umsetzung von TIBER.

Das Ziel ist dabei das Erreichen einer europaweiten Konvergenz, indem mit anderen TCTs zusammengearbeitet und an Aktivitäten des TIBER-EU Knowledge Centre (TKC) der EZB, Schulungen und am laufenden Austausch bewährter Verfahren teilgenommen wird.

Das TCT ist funktionell von der Aufsichtstätigkeit der FMA getrennt.

4.2 Kontaktdaten

Bei Fragen zu TIBER-EU LI steht das TCT der FMA unter folgender E-Mail-Adresse zur Verfügung: TCT@fma-li.li

5. Verweis auf TIBER-EU

Im Rahmen von TIBER-EU LI werden die Dokumente des TIBER-EU Rahmenwerks in der jeweils aktuellen Fassung ohne nationale Anpassung angewendet. Die folgende Webseite beinhaltet einen Gesamtüberblick über sämtliche für TIBER-EU LI relevanten Dokumente:

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

6. Schlussbestimmungen und Inkrafttreten

Diese Mitteilung wurde von der Geschäftsleitung der FMA am 7. Oktober 2025 genehmigt und tritt per 15. Oktober 2025 in Kraft.