

# TIBER-MT and DORA TLPT-MT National Implementation Document

Threat Intelligence-Based Ethical Red Teaming – Malta  
DORA Threat-Led Penetration Testing – Malta

7 July 2025

# Contents

|  |   |
|--|---|
| List of Abbreviations .....                                      | 3 |
| Legal Disclaimer .....   | 4 |
| Chapter 1: Background .....                                      | 5 |
| Chapter 2: Introduction to TIBER-EU .....                        | 5 |
| Chapter 3: Our work with TIBER-EU .....                          | 5 |
| Chapter 4: The relationship between TIBER-EU and DORA TLPT ..... | 6 |
| Chapter 5: Official Statement of Adoption .....                  | 6 |
| Chapter 6: TIBER-MT Overview .....                               | 7 |
| 6.1 TIBER-MT's relation to TIBER-EU .....                        | 7 |
| 6.2 TIBER-MT Authority .....                                     | 7 |
| 6.3 Target Sectors .....   | 7 |
| Chapter 7: Reference to TIBER-EU Framework and Guidance .....    | 8 |

## List of Abbreviations

|                 |  |
|-----------------|--|
| <b>MFSA</b>     | Malta Financial Services Authority                   |
| <b>SIRC</b>     | Supervisory ICT Risk and Cybersecurity               |
| <b>DORA</b>     | Digital Operational Resilience Act                   |
| <b>RTS</b>      | Regulatory Technical Standard                        |
| <b>TIBER-EU</b> | Threat Intelligence-Based Ethical Red Teaming Europe |
| <b>TIBER-MT</b> | Threat Intelligence-Based Ethical Red Teaming Malta  |
| <b>TLPT</b>     | Threat-Led Penetration Testing                       |
| <b>ESCB</b>     | European System of Central Banks                     |
| <b>ECB</b>      | European Central Bank                                |
| <b>SSM</b>      | Single Supervisory Mechanism                         |
| <b>FE</b>       | Financial Entity                                     |
| <b>TCT</b>      | TIBER and TLPT Cyber Team                            |
| <b>TCT-MT</b>   | TIBER and TLPT Cyber Team Malta                      |
| <b>TM</b>       | Test Manager   |

## Legal Disclaimer

This document and its content are intended only for informational purposes. This document is not legal advice, compliance advice, or professional advice. It is not a replacement or interpretative for any acts, regulations, technical standards, rules, frameworks, and guidelines, that are applicable to the Financial Entity. Responsibility shall not be attributed to the Malta Financial Services Authority for any damages incurred by any person arising as a direct result of reliance on any of the content expressed throughout this document.

The “TIBER-MT and DORA TLPT-MT National Implementation Document” is written in accordance with the Framework for Threat Intelligence-Based Ethical Red Teaming published in February 2025, and the Regulation (EU) 2022/2554 on digital operational resilience for the financial sector, alongside the Regulatory Technical Standards (EU) 2025/1190 (the ‘[RTS](#)’) specifying elements related to threat-led penetration tests under Article 26 (11) of the Digital Operational Resilience Act.

The “TIBER-MT and DORA TLPT-MT National Implementation Document” does not apply to credit institutions classified as “[Significant Entities](#)” by the Single Supervisory Mechanism where the European Central Bank is the competent Threat-Led Penetration Testing authority under the Regulation (EU) 2022/2554 on digital operational resilience for the financial sector.

## Chapter 1: Background

TLPT has emerged as a critical measure for bolstering the digital resilience of FEs, driven by the need to simulate realistic and high-impact cyber threats. This enables FEs to identify vulnerabilities and test their response capabilities under conditions similar to those of actual attacks. For certain FEs within the European Union, TLPT is not only best practice but also a regulatory requirement under DORA, which mandates enhanced security and resilience standards to ensure the stability of the financial ecosystem. The updated TIBER-EU Framework, published on 11 February 2025, was established to provide guidance for these entities as well as authorities regarding TLPT, standardising and harmonising how intelligence-led red team tests are performed in the EU and to align the framework with the requirements set out in DORA.

## Chapter 2: Introduction to TIBER-EU

In May 2018, the ECB published the TIBER-EU Framework, the first EU-wide framework for Threat Intelligence-Based Ethical Red Teaming that provided an efficient solution for ensuring mutual recognition of cyber resilience tests across the EU. The framework was jointly developed by the ECB and the EU national central banks aiming to help the entities that formed the core European financial infrastructure to test and enhance their protection, detection, and response capabilities. In February 2025, the ECB updated the TIBER-EU Framework to fully align it with DORA and the respective RTS on TLPT. This framework ensures a qualitative, controlled, and safe TLPT approach across the EU, providing comprehensive guidance for cyber resilience testing and facilitates a uniform and harmonised approach for TLPT for FEs across Europe.

## Chapter 3: Our work with TIBER-EU

In response to the growing reliance on Information and Communications Technology by organisations globally and the recent introduction of the DORA Regulation, TLPT has emerged as a crucial tool for enhancing the digital resilience of FEs. Recognising this, the MFSA launched a public consultation on March 2023, titled "[Consultation on the Adoption of the TIBER-EU Framework in Malta](#)" ('The Consultation').

The Consultation aimed to introduce the TIBER-EU Framework to industry stakeholders, highlighting its alignment with DORA's advanced testing requirements based on TLPT. Additionally, it sought to gather feedback from stakeholders on the potential adoption of the TIBER-EU Framework in Malta. The positive response from the industry was reflected in the "[Feedback statement on the Adoption of the TIBER-EU Framework in Malta](#)", published by the MFSA on February 2024, indicating strong support for the framework's introduction.

Following extensive discussions with the ECB and the release of the latest version of the TIBER-EU Framework on February 2025, the MFSA has officially adopted the TIBER-EU Framework. This adoption is part of the MFSA's ongoing efforts to comply with DORA and to continue strengthening the digital resilience of the Maltese financial sector, culminating in the creation of the "TIBER-MT and DORA TLPT-MT National Implementation Document".

## Chapter 4: The relationship between TIBER-EU and DORA TLPT

Article 26 (11) of the DORA Regulation, which mandates TLPT for FEs, states that the ESA, in agreement with the ECB, shall develop a joint draft RTS in accordance with the TIBER-EU Framework. As of February 2025, the TIBER-EU Framework mirrors the process and structure of TLPT described in the respective RTS, allowing it to be used as guidance on how to complete DORA TLPT for both FEs and national competent authorities. Therefore, after the completion of a test, if the FE was compliant throughout the TIBER-EU process in accordance with the obligations set out in the TIBER-EU Framework and the requirements from DORA TLPT, an attestation is issued. This attestation signifies that the FE is in full compliance with the TIBER-EU Framework, as well as the DORA Regulation and RTS, in relation to the obligations for TLPT. For further information on how the TIBER-EU Framework can help fulfil the DORA requirements for TLPT, it is recommended to read ECB's paper titled "[Adopting TIBER-EU will help fulfil DORA requirements](#)".

For the case of credit institutions classified as "[Significant Entities](#)", as per Article 6 (4) of Council Regulation (EU) No 1024/2013, supervised by the SSM, the ECB is the competent TLPT authority.

## Chapter 5: Official Statement of Adoption

The Malta Financial Service Authority, as the national competent authority within Malta, hereby declares that the TIBER-EU Framework has been implemented into a "TIBER-MT and DORA TLPT-MT National Implementation Document", hereafter referred to as 'the Document', for the Maltese jurisdiction to comply with the Digital Operational Resilience Act ((EU) 2022/2554) regarding Threat-led Penetration Testing. This adoption includes all the core foundational concepts and approaches in the TIBER-EU Framework. Moreover, there are no specific differences between the Document and the TIBER-EU Framework.

## Chapter 6: TIBER-MT Overview

### 6.1 TIBER-MT's relation to TIBER-EU

The TIBER-MT mirrors all the core methodology, phases and deliverables of the TIBER-EU Framework, in the scope to meet the TLPT requirements set out by the DORA Regulation. Therefore, a FE that underwent a TIBER-MT test, shall, if the FE was compliant throughout the TIBER process in accordance with the obligations set out in the TIBER-EU Framework, be issued with a TIBER-MT Attestation at the end of the test. This attestation confirms that the test was conducted in accordance with the requirements, as set out in TIBER-EU Framework.

The TIBER-EU Framework serves as guidance to aid in fulfilling DORA TLPT requirements. Since TIBER-MT mirrors the TIBER-EU Framework, an FE issued a TIBER-MT Attestation may be seen as compliant with DORA TLPT, provided that the mandatory requirements under the DORA Regulation and TLPT RTS are adhered to throughout the TIBER-MT test. For further information on how the TIBER-EU Framework can help fulfil the DORA requirements for TLPT, it is recommended to read ECB's paper titled "[Adopting TIBER-EU will help fulfil DORA requirements](#)".

For further information, in addition to the Document, readers are encouraged to explore the TIBER-EU Framework, other TIBER-EU guidance documents, the DORA Regulation ((EU) 2022/2554), and the respective TLPT RTS.

### 6.2 TIBER-MT Authority

The MFSA is recognised as the TIBER-MT Authority, responsible and accountable for the requirements set out within the TIBER-EU Framework and other resources shared by the ECB.

The [SIRC Function](#) at the MFSA will comprise the staff of the national TCT-MT, which serves the same function as its DORA equivalent. So, the TCT-MT will be the body overseeing the activities of TIBER-MT tests, as outlined in the TIBER-EU Framework. Additionally, the TCT-MT, is comprised of TMs, also sourced from the SIRC Function, for each TIBER-MT test.

**The TIBER-MT Authority, TCT-MT, and TMs can be reached at [tlpt@mfsa.mt](mailto:tlpt@mfsa.mt)**

### 6.3 Target Sectors

The MFSA will use the TIBER-EU/MT documentation as the methodology to complete DORA TLPT tests. Articles 26 of DORA identifies the FEs within the scope of a TLPT. The relevant RTS on TLPT further specifies, as per Article 2 (1), that the TIBER-MT Authority shall assess whether a FE's impact, systemic characteristics, and ICT risk profile to determine if they are required to perform a TIBER-MT test. Additionally, the TIBER-MT Authority shall require the FE listed in Article 2 (2) of the RTS to perform a TIBER-MT test.

Therefore, the target sectors in scope of a TIBER-MT are:

- **Target 1** – FEs licenced by the MFSA that fall within scope of Article 2 (1) of the RTS, emanating from the DORA Regulation ((EU) 2022/2554);
- **Target 2** – FEs licenced by the MFSA, as referred to Article 2 (2) of the RTS, emanating from the DORA Regulation ((EU) 2022/2554).

## Chapter 7: Reference to TIBER-EU Framework and Guidance

Any information used in the creation of the Document for the implementation of the TIBER-EU Framework within the Maltese jurisdiction, as well as additional important resources for the conduct of a TIBER-MT test, can be found here:

| Documentation   | Content   |
|---|---|
| <a href="#">TIBER-EU Framework</a>                                    | How to implement the European Framework for Threat Intelligence-Based Ethical Red teaming.  |
| <a href="#">TIBER-EU Control Team Guidance</a>                        | How relevant stakeholders can set up a Control Team Lead and Control Team.  |
| <a href="#">TIBER-EU Initiation Documents</a>                         | The information on the requirements for the content and format to consider when drafting an Initiation Document.                  |
| <a href="#">TIBER-EU Scope Specification Document Guidance</a>        | The information on the requirements for the goal, content and format of the Scope Specification Document.                         |
| <a href="#">TIBER-EU Guidance for Service Provider Procurement</a>    | Requirements and considerations when procuring the Threat Intelligence Provider and Red Test Team.                                |
| <a href="#">TIBER-EU Targeted Threat Intelligence Report Guidance</a> | The information on the requirements for the content and format to consider when drafting the Targeted Threat Intelligence Report. |
| <a href="#">TIBER-EU RED Team Test Plan Guidance</a>                  | The information on the requirements for the content and format to consider when   |



[TIBER-EU Red Team Test Report Guidance](#)

drafting the Red Team Test Plan.

The information on the requirements for the content and format to consider when drafting the Red Team Test Report.

[TIBER-EU Blue Team Test Report Guidance](#)

The information on the requirements for the content and format to consider when drafting the Blue Team Test Report.

[TIBER-EU Purple Teaming Guidance](#)

Requirements and considerations when conducting Limited Purple Teaming during the testing phase and Purple Teaming during the closure phase.

[TIBER-EU Test Summary Report Guidance](#)

The information on the requirements for the content and format to consider when drafting the Test Summary Report.

[TIBER-EU Remediation Plan Guidance](#)

The information on the requirements for the content and format to consider when drafting the Remediation Plan.

[TIBER-EU Attestation Guidance](#)

The information on the requirements for the content and format to consider when drafting the Attestation.

[Adopting TIBER-EU will help fulfil DORA requirements](#)

A paper on how the TIBER-EU can help and benefit financial entities and authorities to fulfil DORA requirements for TLPT.