MFSA MALTA FINANCIAL SERVICES AUTHORITY

Circular

16 June 2026

Comparing the TIBER-EU Framework with other established Non-EU TLPT Frameworks

Chapter IV of Regulation (EU) 2022/2554 on Digital Operational Resilience for the Financial Sector ('the DORA Regulation') sets out requirements for testers for the carrying out of threat-led penetration testing ('TLPT'), which were subsequently extended within the relevant Regulatory Technical Standard, i.e. Commission Delegated Regulation (EU) 2025/1190 on Threat-Led Penetration Testing ('the RTS').

Article 7 of the RTS requires that TLPT providers, including testers and threat intelligence providers, provide references from previous assignments related to or in the context of penetration testing and red team testing, respectively. However, the European Securities and Markets Authority ('ESMA'), in its Final Report submitted on 17 July 2024, further noted that:

Chapter 1, paragraph 4 "*Respondents appeared to be very concerned with the requirements applying to TLPT providers (both testers and threat intelligence providers), which were mostly deemed too strict considering the limited availability of these providers on the existing market*"

This is reflected by the Bank of Italy, in a paper titled "Exploratory Survey of the Italian Market for Cybersecurity Testing Services" published on 13 May 2026, which identified a shortage of skilled professionals and market concentration as relevant indicators of limited provider depth within the TLPT sector.

The framework for Threat Intelligence-Based Ethical Red-teaming ('TIBER-EU framework') has allowed for voluntary TIBER testing since May 2018. Accordingly, previous experience obtained through TIBER tests may be relevant when assessing compliance with Article 7 of the RTS. Testers and threat intelligence providers may, however, have obtained relevant practical experience through established non-EU TLPT frameworks.

The Malta Financial Services Authority (the 'MFSA', or 'the Authority') felt the need to carry out a comparison between the TIBER-EU framework and other TLPT frameworks established outside of the EU. This comparison is being published in the form of a mapping exercise, titled "Comparing the TIBER-EU Framework with other established Non-EU TLPT Frameworks" (the 'Mapping Exercise'), alongside this circular and can be found online on the Threat-Led Penetration Testing section of the Supervisory ICT Risk and Cybersecurity page within the MFSA website. The Mapping Exercise compares the core components the TIBER-EU framework with other recognised non-EU TLPT frameworks, namely CBEST,

iCAST, AASE, and I-CRT. This document seeks to support Financial Entities, TLPT providers, and relevant competent authorities in assessing whether prior experience obtained under recognised non-EU threat intelligence-led testing frameworks may be considered when demonstrating relevant expertise, capabilities, and previous assignments for the purposes of Article 7 of the RTS on TLPT.

Further information may be requested by sending an email to the TIBER-MT/TLPT Cyber Team within the MFSA through tlpt@mfsa.mt.