MFSA MALTA FINANCIAL SERVICES AUTHORITY

Circular

23 April 2026

MFSA Releases its Guidance Supporting the Development of Codes of Conduct by Financial Entities and TLPT Providers in Line with Regulation (EU) 2022/2554 for the carrying out of Threat-Led Penetration Testing

The Malta Financial Services Authority ('MFSA', 'the Authority') is designated as the Threat-Led Penetration Testing ('TLPT') Authority for Threat-Led Penetration Tests carried out under the Digital Operational Resilience Act ('the DORA Regulation') (Regulation (EU) 2022/2554) and the relevant Regulatory Technical Standard, i.e. Commission Delegated Regulation (EU) 2025/1190 on Threat-Led Penetration Testing ('the RTS') within the Maltese Jurisdiction.

Chapter IV of the DORA Regulation on Digital Operational Resilience Testing, specifically Article 27, sets out the requirements for Testers, either internal or external to the financial entity ('FE'), carrying out of TLPT; which was subsequently extended with the RTS to include Threat Intelligence Providers. In line with this, Article 27, specifically the first paragraph, sets out, among other requirements that FEs' identified to carry out advanced testing by means of TLPT at least every three years shall only use Testers that:

> "*(c) are certified by an accreditation body in a Member State or adhere to formal codes of conduct or ethical frameworks;*"

This requirement is cross-referenced in the Article 9(11) of the RTS, which necessitates that both Testers and Threat Intelligence Providers comply with the requirements laid down in Article 27 of the DORA Regulation and with Article 7(1) of the RTS before an FE may commence procurement for a TLPT engagement.

Therefore, to supplement the obligation referenced in DORA Article 27(1)(c), the MFSA initiated a collaboration with the TIBER-EU Knowledge Centre ('TKC') to develop guidance outlining recommendations and best practices for the development of core principles of such codes of conduct. This collaboration resulted in the publication of the "TLPT Codes of Conduct Guidance Document" (the 'Guidance Document').

The Guidance Document is aimed at TLPT providers, including ICT third-party service providers contracted as external Testers and Threat Intelligence Providers for TLPT, as well as FEs when internal Testers are selected. Its purpose is to provide guidance to these entities in developing their own Code of Conduct, thereby enhancing the suitability of external Testers and Threat Intelligence Providers, as well as internal Testers of FEs, to

carry out TLPT through the European framework for Threat Intelligence-Based Ethical Red Teaming ('TIBER-EU framework'). This guidance applies to both natural persons and legal bodies responsible for providing or staffing Testers and/or Threat Intelligence Providers.

FEs licenced by the MFSA, as well as Testers and Threat Intelligence Providers, are strongly encouraged to review the Guidance Document for further information.

> To reach the TIBER-MT Authority, kindly contact the Maltese TIBER/TLPT Cyber Team within the MFSA through tlpt@mfsa.mt.

For further information, kindly go to the Threat-Led Penetration Testing section of the Supervisory ICT Risk and Cybersecurity page within the MFSA website.