MFSA MALTA FINANCIAL SERVICES AUTHORITY

TLPT Codes of Conduct Guidance Document

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

CONTENTS

REVISIONS LOG

VERSION	DATE ISSUED	DETAILS
1.00	23 April 2026	Document Issued

1. Introduction

Threat-Led Penetration Testing ('TLPT') has emerged as a critical measure for bolstering the digital resilience of financial entities ('FEs'), driven by the need to simulate realistic and high-impact cyber threats. Unlike traditional penetration testing, TLPT mirrors real-life tactics, techniques, and procedures of sophisticated threat actors. 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 the Digital Operational Resilience Act Regulation (EU) 2022/2554 (the 'DORA Regulation'), which mandates enhanced security and resilience standards to ensure the stability of the financial ecosystem.

As one of the requirements set out in Article 27(1) of the DORA Regulation, TLPT providers must either be certified by an accreditation body in a Member State or adhere to formal Codes of Conduct or ethical frameworks. In support of this, the Malta Financial Services Authority initiated a collaboration with the TIBER-EU Knowledge Centre ('TKC') to develop guidance outlining expectations and best practices for the construction of core principles of such Codes of Conduct.

1.1. Purpose of this document

This document is intended to provide guidance on the creation of a Code of Conduct that enhances the suitability of TLPT 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').

1.2. Target Audience

This guidance document is aimed at TLPT providers, including ICT third-party service providers ('ICT TPPs') contracted as external testers and threat intelligence providers ('TI 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, targeting their staff for red teaming, threat intelligence ('TI'), or both. The guidance applies to both natural persons and legal bodies responsible for providing or staffing testers and/or TI providers.

2. Definitions

Competent authority	The TLPT authority and/or TIBER authority
Critical or important function ('CIF')	A function, the disruption of which would materially impair the financial performance of a FE, or the soundness or continuity of its services and activities, or the discontinued, defective or failed performance of that function would materially impair the continuing compliance of a FE with the conditions and obligations of its authorisation, or with its other obligations under applicable financial services law, (DORA, Article 3(22))
DORA Regulation (EU) 2022/2554 ('DORA')	Regulation (EU) 2022/2554 of the European Parliament and of the council of 14 December 2022 on digital operational resilience for the financial sector and amending regulations (EU) no 1060/2009, (EU) no 648/2012, (EU) no 600/2014, (EU) no 909/2014 and (EU) 2016/1011
Financial entity ('FE')	The entities identified under Article 26 (1) of the DORA Regulation (EU) 2022/2554, and further specified in Article 2 of the RTS (EU) 2025/1190, required to undergo TLPT
Flag	The objective defined for each scenario that the testers have the goal to capture during the test, (TIBER-EU framework)
GDPR (EU) 2016/679 ('GDPR')	Regulation (EU) 2016/679 of the European Parliament and of the council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC
ICT intra-group service provider	An undertaking that is part of a financial group and that provides predominantly ICT services to FEs within the same group or to FEs belonging to the same institutional protection scheme, including to their parent undertakings, subsidiaries, branches or other entities that are under common ownership or control, (DORA, Article 3(20))
ICT third-party service provider ('ICT TPP')	An undertaking providing ICT services, (DORA, Article of 3(19))

Leg-up	The assistance which may be needed during active testing by the testers, such as network, and/or system accesses, and/or devices, to achieve a scenario for testing, for the sake of time and resources in a given TLPT and/or a TIBER test, (TIBER-EU framework)
Regulatory Technical Standard (EU) 2025/1190 (the 'RTS')	Commission Delegated Regulation (EU) 2025/1190 supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying the criteria used for identifying FEs required to perform TLPT, the requirements and standards governing the use of internal testers, the requirements in relation to scope, testing methodology and approach for each phase of the testing, results, closure and remediation stages and the type of supervisory and other relevant cooperation needed for the implementation of TLPT and for the facilitation of mutual recognition
Testers	Externally contracted providers or designated individuals within the FE subject to TLPT and/or a TIBER test, that carries out a simulated attack by attempting to compromise the critical functions of the FE, mimicking a cyber-attacker in accordance with the respective DORA Regulation and TIBER-EU framework. This definition shall refer to both natural persons and legal bodies responsible for providing or staffing testers
Threat-Led Penetration Testing ('TLPT')	A framework that mimics the tactics, techniques, and procedures of real-life threat actors perceived as posing a genuine cyber threat, and that delivers a controlled, bespoke, intelligence-led (Red Team) test of the FE's critical live production systems, (DORA 2022/2554)
Threat intelligence ('TI')	Information that has been aggregated, transformed, analysed, interpreted or enriched to provide the necessary context for decision-making and to enable relevant and sufficient understanding in order to mitigate the impact of an ICT-related incident or of a cyber threat, including the technical details of a cyber-attack, those responsible for the attack and their modus operandi and motivations
Threat intelligence providers ('TI providers')	The expert(s), contracted by the FE for each TLPT, and external to the FE, who collect and analyse targeted TI relevant for the FE in scope of a specific TLPT exercise

	and develop matching relevant and realistic threat scenarios, (RTS, Article 1(10)). This definition shall refer to both natural persons and legal bodies responsible for providing or staffing TI providers
Threat scenario	A description of the end-to-end attack path based on the identified threat profiles
TIBER Cyber Team ('TCT')	The staff within the TIBER authority, that is responsible for TIBER-related matters, (TIBER-EU framework)
TIBER-EU framework	An EU-wide framework for Threat Intelligence-Based Ethical Red Teaming published by the European Central Bank ('ECB') that delivers a controlled, bespoke, intelligence-led Red Team test of entities' critical live production systems
TIBER-Knowledge Centre ('TKC')	A forum hosted by the ECB in which national and European TIBER-EU cyber teams coordinate and discuss initiatives and share details of their experiences
TIBER authority	Any authority under the TIBER framework and/or its national or European implementations, conducting (regulatory) tasks within a TIBER test. They are responsible for adopting and implementing TIBER-EU, closely monitoring and guiding the test and ensuring it is conducted in the right spirit and in accordance with the requirements of the TIBER-EU framework, (TIBER-EU framework). When using the TIBER-EU framework for TLPT obligations under DORA, the respective "TLPT authorities" are considered as TIBER authorities for that test
TIBER test	A test conducted using the TIBER-EU framework, which the FE may use to assess their critical live production systems resilience against sophisticated cyber threats in a controlled environment, (TIBER-EU framework)
TLPT authority	a. the single public authority in the financial sector designated in accordance with Article 26(9) of Regulation (EU) 2022/2554, or; b. the authority in the financial sector to which the exercise of some or all of the tasks in relation to TLPT is delegated in accordance with Article 26(10) of Regulation (EU) 2022/2554, or;

	c. the competent authority in accordance with Article 46 of Regulation (EU) 2022/2554, (RTS, Article 1(7)). As mentioned in the RTS, the European Central Bank is the designated TLPT authority and TIBER authority for Credit institutions classified as significant, in accordance with Article 6(4) of Regulation (EU) No 1024/2013
TLPT providers	The testers and threat intelligence providers within a TLPT, (RTS, Article 1(11))
Traffic Light Protocol 2.0 (TLP+)	A system of markings that designates the extent to which recipients may share potentially sensitive information

3. Core Principles

A Code of Conduct for TLPT providers is recommended to contain core principles which aim to:

1. Clarify the ethical standard expected from TLPT providers, both prior to and following the engagement for testing activities.
2. Define the expected behaviour and responses of TLPT providers during testing activities.
3. Establish the standard for reporting, record keeping, and information exchange level required of TLPT providers.
4. Assess the suitability of TLPT providers, whether involved as members of a corporate body, partnership, or shareholder, in relation to the FE's risk appetite and the broader context of the financial sector.
5. Respect and uphold the intellectual property right.

By adhering to these core principles, the TLPT providers will provide assurance to the FE and the competent authority regarding their professional conduct, both as the legal body and the natural persons representing it. However, the determination of which types of principles are to be included in the Code of Conduct remains at the discretion of the TLPT providers.

In addition to adhering to the Codes of Conduct, the TLPT providers should comply with all applicable acts, regulations, technical standards, rules, frameworks, and guidelines. This includes the TIBER-EU framework, DORA Regulation (EU) 2022/2554 Level 1 and Level 2 texts, particularly the Regulatory Technical Standard on TLPT (EU) 2025/1190 (the 'RTS'), the General Data Protection Regulation (EU) 2016/679 ('GDPR'), and any other relevant national laws of the respective EU Member State.

Moreover, the provisions outlined in this document and when drafting one's own Code of Conduct should be without prejudice to the TIBER-EU framework and its TIBER-EU local implementation, DORA Regulation (EU) 2022/2554 Level 1 and Level 2 texts, particularly the Regulatory Technical Standard on TLPT (EU) 2025/1190 (the 'RTS'), the General Data Protection Regulation (EU) 2016/679 ('GDPR'), and any other applicable acts, regulations, technical standards, rules, contracts, frameworks, guidelines, or other codes of conduct.

3.1. Ethical Conduct

A principle on the ethical conduct of TLPT providers is important within a Code of Conduct as it lays down the expected and appropriate behaviour within a particular test. Therefore, as best practices, this principle should encompass the following:

3.1.1. Engagement of parties

The TLPT providers shall not associate with malicious hackers, except where such association is legally required for the fulfilment of their duties. They shall also refrain from engaging in any malicious activities that may endanger the FE, its ICT TPPs or ICT intra-group service providers involved, or any other stakeholder.

3.1.2. Evaluation of Security Tools

The TLPT providers shall not knowingly use software or process that is obtained or retained either illegally or unethically, except where such use is legally required for the fulfilment of their duties.

3.1.3. Conflict of interest

The TLPT providers shall disclose to the FE and competent authority(ies) any level of bias in relation to the FE, ICT TPP, or an ICT intra-group service provider involved in TLPT. Conflicts of interest include, but are not limited to, the following:

(a) The TLPT providers are directly or indirectly linked by way of control to the FE resulting in a likelihood of financial gain or avoidance of a financial loss;

(b) The TLPT providers having direct or indirect ownership interest, financial stake, or controlling influence shared with any key individual within the FE;

(c) The TLPT providers or FE have an interest in the outcome of the test, distinct from the scope of a TIBER test;

(d) The TLPT providers or FE receives or will receive an inducement in relation to the TIBER test, in the form of monies, goods or services, other than the commission or fee from that service of the test;

(e) The TLPT providers have provided consultancy, advisory, or similar services to the FE, outside the scope of TLPT, which could influence the TLPT providers' objectivity during the test;

(f) The TLPT providers have an undisclosed interest in products and/or services which they may recommend to the FE;

(g) The TLPT providers have performed BT tasks or other services that may present a conflict of interest to the FE, ICT TPP, or an ICT intra-group service provider, during periods of suspension of the test.

3.1.4. Certification Integrity

In order to uphold the highest standards of professionalism, integrity, and trust within the providing of TI, testing, and certification environment, the following principles shall apply:

(a) the TLPT providers shall act with honesty in obtaining any certifications, ensuring that the integrity of the examination environment is upheld and not compromised. They must refrain from engaging in misconduct that could undermine the integrity or confidentiality of the certification process;

(b) the TLPT providers shall not make misleading use of certificates, marks, or logos in any publications, catalogues, documents, or public communications, including speeches. Moreover, TLPT providers shall refrain from promoting any certification that has been withdrawn or suspended;

(c) the TLPT providers shall ensure that any certifications they declare in their CVs, profiles, or other professional materials are accurate and up to date. If a certification requires periodic recertification and the TLPT provider has not yet recertified, this must be clearly indicated wherever the certification is advertised. Misrepresentation of certification status is not permitted, as it may compromise trust in the integrity of the testing process;

(d) the TLPT providers shall disclose any limitations or restrictions related to their certifications, such as jurisdiction, scope, or expiration, to ensure transparency.

3.1.5. Global Organisations

The TLPT providers who are required to perform TIBER tests outside their parent jurisdiction, the EU, or in collaboration with non-EU states, particularly where the competent authorities have their own Code of Conduct, must ensure they understand and comply with the applicable regulations of the relevant jurisdictions. It is essential that TLPT providers are fully aware of and adhere to the legal and ethical standards governing testing activities in those regions.

3.1.6. Transparency

The TLPT providers shall maintain transparency during the TIBER test, not only with the FE but also with the competent authority(ies), as follows:

(a) they shall not misrepresent or withhold information about the performance of products, tools, systems, or services, except where bound by confidentiality, nor exploit others' lack of knowledge or experience to mislead or misrepresent;

(b) they shall act independently and objectively throughout the TIBER test. Furthermore, if they become aware of any unlawful actions by the FE, ICT TPPs,

or its ICT intra-group service provider, the TLPT providers are obligated to report such actions to the competent authority(ies). In addition, if these unlawful actions constitute a breach of any applicable laws, the respective authority(ies) must be contacted without delay.

3.1.7. Technical competencies

The TLPT providers must continuously develop, refine, and maintain their technical competencies. They must keep up to date with technological advances through training, technical publications, and specialist groups within professional bodies.

3.2. Testing Activity

A TIBER test simulates a real-life intrusion attempt to generate meaningful insights. Therefore, considerations pertaining to the confidentiality, integrity, and availability of testing activities should be encompassed within this principle, as outlined in the best practices below:

3.2.1. Limitations of Scope and Methods

The TLPT providers shall only operate in the scope documented in the TIBER test, agreed with the FE and the competent authority(ies). Therefore, the TLPT providers shall only use methods of testing delineated within the relevant TIBER test.

3.2.2. Respect for fundamental rights and values

The TLPT providers must not engage in any activities that constitute unlawful or unethical behaviour, including but not limited to blackmail, extortion, or coercion. Social engineering activities such as phishing are permitted only if they are explicitly authorised in the agreed scope of work, are conducted in a controlled manner, and do not cause unjust or disproportionate harm to the client, its employees, or third parties. All interactions must respect the dignity, safety, and legal rights of individuals, and must avoid creating lasting negative consequences beyond the objectives of the engagement.

3.2.3. Time commitments and planning

The TLPT providers must proactively manage their workload to ensure that other work or projects do not impede the necessary time and focus required for testing activities. Additionally, the relevant testers shall ensure timelines mapped to the flags and goals are both timely and achievable.

3.2.4. Excellence and continuous improvement

The relevant testers shall demonstrate creative and unique tactics, techniques, and procedures during active testing to avoid repeated use of the same attack paths or overreliance on leg-ups, while still adhering to the scope of the threat scenarios.

3.2.5. Indiscriminate data collection

The TLPT providers shall collect only the data that is relevant to the defined scope of the TIBER test and the threat scenarios.

3.2.6. Avoidance of disruptions during testing activities

Active testing will be conducted on several or all CIFs within a FE's live production systems supporting these functions and, where applicable, on CIFs that are outsourced or contracted to ICT TPPs, therefore:

(a) the relevant testers shall not intentionally cause disruption during active testing, including but not limited to the deletion of data, interruption of server uptime, or any actions that could negatively impact system availability or integrity

(b) the relevant testers shall proactively create and implement measures to avoid the disruptions as a result of their active testing.

3.2.7. Alerting

The TLPT providers shall, upon discovering a significant security vulnerability or encountering a real intrusion or attempt, immediately cease all current activities and notify the FE and the competent authority(ies) without delay.

3.2.8. Clean-up activities

The relevant testers, after the completion of active testing, are required to perform restoration procedure to safeguard the integrity of the tested entity's environment. Therefore:

(a) the relevant testers shall execute these procedures with the utmost care, ensuring a thorough cleanup of all artifacts and information introduced during the testing process.

(b) the relevant testers shall confirm with the FE that no residual elements remain which could potentially impact the integrity or security of the tested environment.

3.3. Reporting, Record Keeping, & Information Exchange

Written deliverables are a consistent outcome of a TIBER test. Therefore, a principle outlining the expected standard should be included in a Code of Conduct to support a shared understanding among relevant stakeholders, as reflected in the best practices below:

3.3.1. Language
The TLPT providers shall present verbal or written deliverables in the common language to the relevant stakeholders of the TIBER test.

3.3.2. Legibility
The TLPT providers shall ensure that all information is communicated clearly, using proper language and grammar, clear figures and diagrams, and presented in a manner that is understandable to both technical and non-technical stakeholders of the TIBER test.

3.3.3. Accountability
The TLPT providers shall maintain accountabilities for all actions undertaken during active testing. This accountability must be clearly reflected in both verbal and written deliverables.

3.3.4. Classification
The TLPT providers shall clearly label the security level of all reports, plans, documentation, and material produced, whether in electronic or physical form, according to the TLP+.

3.3.5. Processing
The TLPT providers shall maintain a control list documenting all processing activities involving data collected during the TIBER test. This includes any transfers, report writing, and other iterations of the data where the level of granularity or content could potentially lead to the identification of the source.

3.4. Suitability

The entity responsible for TLPT providers should be expected to disclose any risks associated with the testers and providers assigned to the TIBER test. Therefore, as a best practice, it is recommended that a principle addressing the following be included in a Code of Conduct:

3.4.1. Integrity
In order to assess the integrity of TLPT providers, whether involved as members of a corporate body, partnership, or shareholder, they shall disclose to the FE and competent authority(ies) the following:

(a) the TLPT providers who, in any jurisdiction, been dismissed or asked to resign and did resign from any profession, vocation, office or employment, or from any position of trust or fiduciary appointment, whether or not remunerated, due to misconduct, breach of duty, or any conduct reflecting adversely on their integrity, competence, or fitness for such role;

(b) the TLPT providers who had a registration, authorisation, and/or membership refused, revoked, withdrawn, terminated or expelled by a Regulatory Authority, government, or by a professional body or association, except where such action was on a voluntary basis or due to the natural expiration of its term;

(c) the TLPT providers who have been barred from entry to any profession or occupation in relation to cyber security;

(d) the TLPT providers who have been sanctioned, censured, reprimanded, disciplined, or publicly criticised by any court of law, tribunal, regulatory or public authority, officially appointed enquiry, university or other educational institution, professional body, or trade association, in relation to previous digital operational resilience testing programmes, such as those carried out under Article 25 of DORA, TLPT and/or TIBER tests;

(e) the TLPT providers who have been subject to regulatory disciplinary measures or actions, including disqualification from a position of trust;

(f) the TLPT providers who have had a licence for testing which was revoked, restricted or suspended to carry on a business activity for which the licence was issued, except where such action was on a voluntary basis or due to the natural expiration of the licence;

(g) the TLPT providers who have been found guilty of conducting or been investigated for possible conduct of any licensable activities without the necessary licence, authorisation or permits;

(h) the TLPT providers who have been, and are not currently, subject to any investigation, nor are they aware of any potential action that might be taken against them by a governmental, public authority, professional, or other regulatory body. Additionally, they have not resigned while under investigation;

(i) the TLPT providers who have had proceedings, as referred to in this section, settled out of court or through the framework of alternative dispute resolution;

(j) the TLPT providers who have been found in breach of any regulations, nor have they been convicted of any offence, criminal or otherwise, by any tribunal or court, in relation to previous digital operational resilience testing programmes, such as those carried out under Article 25 of DORA, or involving TLPT and/or

TIBER tests. This includes convictions under appeal, any formal notification of investigation, or committal for trial;

(k) the TLPT providers who have been, nor are they currently, the subject of any criminal or civil investigations, proceedings, and litigation;

(l) the TLPT providers who have been adjudged by a court to be liable for any fraud, forgery, or other misconduct toward any company in which they are or were involved;

(m) the TLPT providers who have been ever subject to any specific deliberations regarding any aspects of their reputation, in relation to previous digital operational resilience testing programmes, such as those carried out under Article 25 of DORA, or involving TLPT and/or TIBER tests;

(n) the TLPT providers who have had any contractual impediments or restrictions through any previous occupation or employment which preclude them in any way from taking up the proposed position;

3.5. Intellectual Property

Protecting intellectual property is considered a best practice and should be included in a Code of Conduct, as outlined below:

3.5.1. Intellectual property rights

The TLPT providers must respect and uphold the intellectual property rights of others, including but not limited to copyrights, patents, trademarks, trade secrets, and proprietary information. Specifically:

(a) The TLPT providers must not have been found guilty of, or been investigated for, the unauthorised use, theft, or misappropriation of intellectual property, including software, tools, or other assets belonging to third parties or former employers;

(b) The TLPT providers must not have improperly disclosed or misused confidential information or trade secrets obtained in the course of their professional activities;

(c) The TLPT providers must ensure that their work is original or properly licensed, and that they have the necessary rights or permissions to use any third-party intellectual property involved in their testing activities;

(d) The TLPT providers must not knowingly engage in activities that infringe upon the intellectual property rights of others;

(e) The TLPT providers must appropriately credit the intellectual property of others when used or referenced in their work;

(f) The TLPT providers must comply with all intellectual property clauses in contracts, agreements, or licenses they are bound by, including those from previous employment or engagements;

4. Conclusion

This document provides a comprehensive guide for TLPT providers, including ICT TPPs contracted as external testers and TI providers for TLPT, as well as FEs where internal testers are selected, to create their own Code of Conduct applicable to both natural persons and legal bodies, outlining standards based on the five core principles:

1. Ethical Conduct,
2. Testing Activities,
3. Reporting, Record Keeping, & Information Exchange,
4. Suitability, and
5. Intellectual Property.

The upholding of these principles should be paramount in fostering amicable relationships between the TLPT providers, FEs, and the competent authority, both during and after the TIBER test.

Through ethical conduct, TLPT providers can assure the FE and the competent authority during the TIBER test contracting process, enabling proper evaluation as well as fostering a relationship built on trust. The goal of a TIBER test is to simulate a real intrusion or attempt in order to derive meaningful insights. However, if testing activities begin to compromise confidentiality, integrity, or availability, it undermines the very spirit and objective of the test. A structured approach when reporting, record keeping, and information exchange further enhances the insights gained and deepens the knowledge extracted from the TIBER test. Moreover, as risk becomes an increasingly important tool in decision-making, assessing the suitability of TLPT providers is essential to align with the evolving risk tolerance of FEs. Finally, it is important for TLPT providers to respect intellectual property rights when performing a TIBER test.

By implementing the core principles outlined in this guidance, TLPT providers, whether ICT TTPs and/or FEs, commit to the TIBER test's sustained success and positive impact on the FE, the competent authority, and the financial services industry as a whole.

Malta Financial Services Authority

Triq L-Imdina, Zone 1

Central Business District, Birkirkara, CBD 1010, Malta

communications@mfsa.mt

www.mfsa.mt