MFSA MALTA FINANCIAL SERVICES AUTHORITY

Feedback Document

Feedback Statement on the Adoption of the TIBER-EU Framework in Malta

Ref: 03-2023

Date: 6 February 2024

Contents

Acronyms

DORA	Digital Operational Resilience Act (Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector).
ECB	European Central Bank.
GTL	Generic Threat Landscape.
RT	Red Team.
TCT	TIBER Cyber Team.
TI	Threat Intelligence.
TIBER-EU	A European framework for Threat Intelligence-based Ethical Red Teaming. Any reference to the TIBER-EU framework herewith refers to the ECB TIBER-EU framework available on the ECB website on the date of this document (see the *References* section).
TKC	TIBER-EU Knowledge Centre.
TLPT	Threat-Led Penetration Testing.
TTP	Tactics, Techniques and Procedures.

1. Introduction

On 8 March 2023, the Malta Financial Services Authority ('MFSA', 'the Authority') published a Consultation Document on the Adoption of the TIBER-EU Framework in Malta ('the Consultation Document'). The consultation was issued to firstly introduce the TIBER-EU framework to interested industry stakeholders as well as the relationship between its requirements and the requirements of DORA on advanced testing based on TLPT. Secondly, this consultation sought to gather the views of industry stakeholders on the adoption of the TIBER-EU framework in Malta. Annex A illustrates the questions of the consultation.

During the consultation period, expiring on 6 April 2023, the MFSA received various feedback from the industry for the Authority's consideration. This feedback was received from financial entities interested in advanced testing, organisations interested in providing Threat Intelligence and/or Red Team services under the TIBER-EU framework and/or DORA advanced testing based on TLPT, and from entities that provide support to regulators and other authorities to adopt the TIBER-EU framework. The distribution of respondents by respondent type can be found in Figure 1 below.

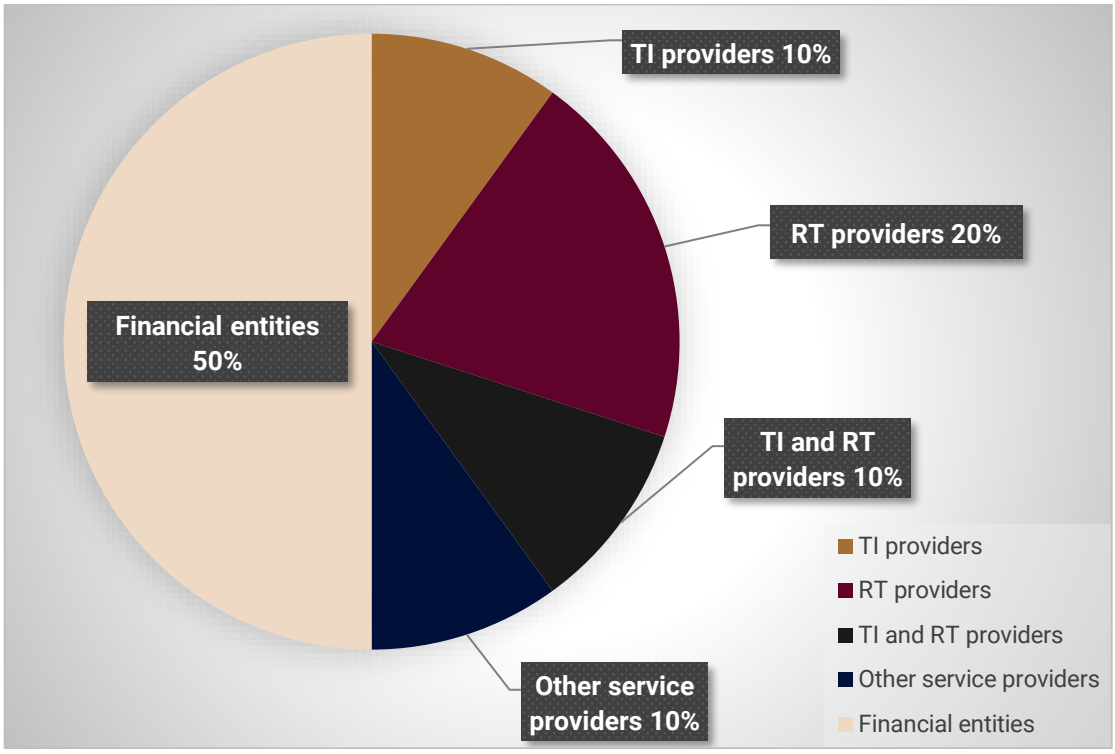


Figure 1: Consultation responses by respondent type

The MFSA reviewed the feedback received and the outcome can be found in Section 3. The feedback has been categorised as follows:

1. Industry views on Threat-Lead Penetration Testing;
2. Industry views on the TIBER-EU framework;
3. Industry views on the introduction of the TIBER-EU framework in Malta (TIBER-MT);
4. Entities in scope of advanced testing based on TLPT and/or the TIBER-EU framework;
5. Internal testers;
6. Internal capabilities required by financial entities;
7. Providing Threat Intelligence and/or Red Team services;
8. Participation in industry fora, groups and networks;
9. Other feedback;
10. MFSA feedback to queries from the industry.

Each feedback category is covered in a dedicated sub-section – sub-sections 3.1 to 3.10 – within Section 3.

Some updates on recent regulatory developments in relation to the DORA Regulation and TIBER-EU have been outlined in Section 2 of this Feedback Statement.

2. Regulatory Developments

2.1 DORA

As per Circular titled Regulation (EU) 2022/2554 and Amending Directive (EU) 2022/2556 on Digital Operational Resilience for the Financial Sector published on the EU Official Journal, the DORA Regulation is to be technically supplemented by a series of Level 2 technical standards with delivery deadlines in January 2024 (hereinafter referred to as the 'first set of Level 2 measures') and July 2024 (hereinafter referred to as 'second set of Level 2 measures').

As informed via Circular titled ESAs Joint Committee Public Consultation on the First Set of Technical Standards under Regulation (EU) 2022/2554 on Digital Operational Resilience for the Financial Sector, the European Supervisory Authorities ('ESAs') have carried out a public consultation on the first set of Level 2 measures. The ESAs have considered the feedback gathered via the public consultation and have delivered the first set of Level 2 measures to the European Commission, as outlined in Circular titled First Set of Technical Standards under Regulation (EU) 2022/2554 on Digital Operational Resilience for the Financial Sector Submitted to the European Commission.

The second set of Level 2 measures, which include the Regulatory Technical Standards specifying elements related to Threat-Led Penetration Testing (Article 26 (11) of DORA), is currently open for public consultation until 4 March 2024, as informed via Circular titled ESAs Joint Committee Public Consultation on the Second Set of Technical Standards under Regulation (EU) 2022/2554 on Digital Operational Resilience for the Financial Sector. The Consultation Paper on Draft Regulatory Technical Standards specifying elements related to Threat-Led Penetration Testing provides further insight on the approach followed in relation to the differences between TIBER-EU and DORA TLPT. Interested stakeholders are invited to refer to sections 3.2.2 and 3.2.3 of the Consultation Paper mentioned above for further guidance. This Level 2 text is still in draft format, and it is subject to changes following feedback from the public consultation.

In relation to the national legal implementation of the DORA Regulation, the Authority has released a Consultation Document on the National Implementation of Regulation (EU) 2022/2554 and Transposition of Directive (EU) 2022/2556 on Digital Operational Resilience for the Financial Sector. Views on the proposed legal measures required for the implementation of the DORA Regulation and transposition of the DORA Amending Directive can be shared with the Authority by 16 February 2024.

2.2 TIBER-EU Framework

A revision of the current TIBER-EU framework, aligned with the respective DORA Consultation Paper on Draft Regulatory Technical Standards specifying elements related to Threat-Led Penetration Testing (still under public consultation as at the date of this document) is expected to be released in due course.

3. Feedback Statement

3.1 Industry Views on Threat-Lead Penetration Testing

This sub-section addresses questions Q1.1 to Q1.4 of the Consultation Document, in which the Authority explored the industry experience in the field of TLPT and the benefits, risks, opportunities, challenges encountered, and any lessons learned by respondents from this experience.

3.1.1 Financial entities' views on TLPT

The practical experience of financial entities in advanced security testing is limited but some entities are exploring the possibility of embedding principles from TLPT and/or the TIBER-EU framework within their future

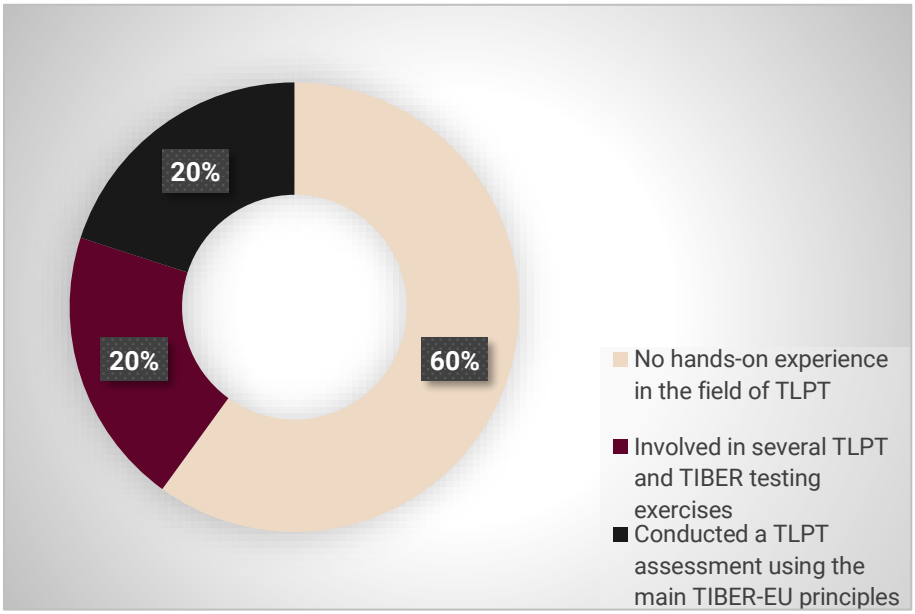


Figure 2: Financial entities' views on TLPT

3.1.2 Service providers' views on TLPT

All responding service providers stated that they have extensive knowledge and/or relevant experience in the field of penetration testing and/or TLPT, including TLPT delivered under various regulatory or non-regulatory frameworks (TIBER, CBEST[1], CREST[2], AASE[3], iCAST[4], CORIE[5]). TLPT is considered to be a wide cyber resilience assessment tool, and therefore able to provide a very accurate improvement plan for entities.

[1] CBEST is a Bank of England and Prudential Regulation Authority's supervisory toolkit to assess the cyber resilience of firms' important business services https://www.bankofengland.co.uk/financial-stability/operational-resilience-of-the-financial-sector/cbest-threat-intelligence-led-assessments-implementation-guide)

[2] CREST Simulated Targeted Attack and Response (STAR) is a framework developed by CREST, an international non-profit, membership body representing the global security industry, to deliver controlled, bespoke, intelligence-led cyber security testing https://www.crest-approved.org/certification-careers/cyber-security-disciplines/

[3] Read Team: Adversarial Attack Simulation Exercises (AASE) is a framework issued by The Association of Banks in Singapore for the financial industry in Singapore https://abs.org.sg/docs/library/abs-red-team-adversarial-attack-simulation-exercises-guidelines-v1-06766a69f299c69658b7dff00006ed795.pdf

[4] Intelligence-led Cyber Attack Simulation Testing (iCAST) is one of the components of the Cyber Resilience Assessment Framework (C-RAF), a risk-based framework issued by the Hong Kong Monetary Authority for Authorized Institutions in Hong Kong, to assess their own risk profiles and benchmark the level of defence and resilience that would be required to accord appropriate protection against cyber-attacks https://www.hkma.gov.hk/eng/news-and-media/press-releases/2020/11/20201103-4/

[5] Cyber Operational Resilience Intelligence-led Exercises (CORIE) is a regulatory framework introduced by the Australian Council of Financial Regulators to improve cyber security resiliency in the Australian financial system https://www.cfr.gov.au/publications/policy-statements-and-other-reports/2022/revised-corie-framework-rollout/pdf/corie-framework.pdf

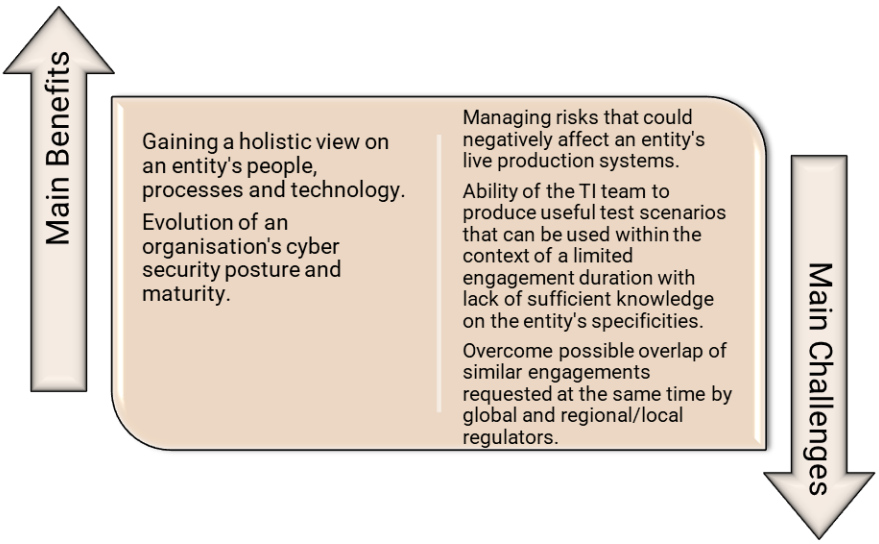


Figure 3: Service providers views on TLPT

TLPT could facilitate the enhancement of the most critical financial entities within a given financial system, in terms of their level of maturity of detection and response capabilities and thus contributing to financial stability.

Some service providers mentioned that during their first TLPT, some financial entities observed that they had very limited visibility of potential adversaries on their network, whereas financial entities that regularly perform such tests, develop better visibility and detection capabilities. In both cases, the assessments seem to provide interesting value and a path for further improvement. TLPT delivered outside any framework seem to be commissioned by entities with a higher level of cyber-maturity who seek primarily to improve their capabilities rather than ensuring compliance with any specific regulation. These kinds of engagements tend to be more flexible/customisable and more financially competitive compared to TIBER-EU assessments.

3.1.3 TLPT benefits and opportunities as seen by service providers

Understanding entities' internet footprint and how publicly available information and systems can be used by attackers to target them.	Very positive customer experience with a very large list of lessons learnt, improvement opportunities, training to the Blue Team, and overall greater visibility and understanding of the resilience of an entity against sophisticated attacks.	Assessing the effectiveness of the entities' monitoring and incident response processes, very close to what would happen in real cyber-attacks.
Assessing the effectiveness of security controls at the perimeter, in the internal corporate network and cloud infrastructures.	Testing the level of employee security awareness against real-world attacks.	Increasing awareness of real-life tactics, techniques, and procedures (TTPs) across different technology verticals of the entities and a better understanding of cyber risks by senior management.

Figure 4: TLPT Benefits and opportunities as seen by service providers

3.2 Industry Views on the TIBER-EU Framework

This sub-section addresses questions Q2.1 to Q2.3 of the Consultation Document, in which the Authority explored the experience related to the TIBER-EU framework and the benefits, risks, opportunities, challenges encountered, and any lessons learnt by respondents from this experience.

3.2.1 Financial entities' views on the TIBER-EU framework

The responding financial entities' experience with TIBER exercises is limited. However, it was noted that the entities involved in such assessments obtained valuable insights regarding their defence in depth approach.

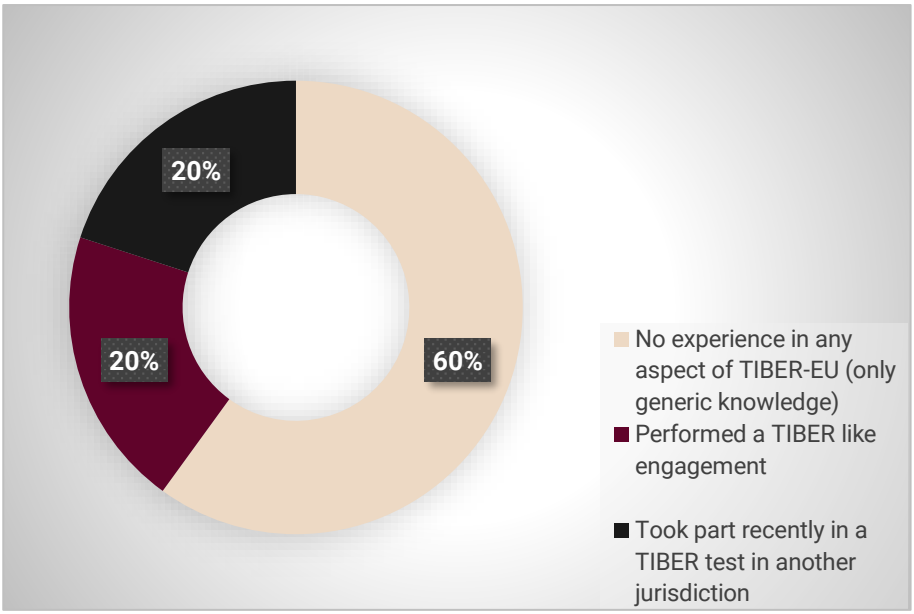


Figure 5: Financial entities' experience in the field of TIBER-EU

Challenges encountered by financial entities involved in TIBER (like) exercises	Gathering intelligence on specific threats for the Maltese financial sector.
	Preparing the test without the knowledge of the security team in charge with the entity's protection (the blue team).
	Continuing the test when a particular control is hard to be bypassed by the Red Team.
	Documenting the testing activities to produce a proper test report, readable by management, at the end of the test.

Figure 6: Challenges in TIBER (like) exercises

3.2.2 Service providers' views on the TIBER-EU framework

The responding service providers see the TIBER-EU framework as a comprehensive, well-structured approach for conducting TLPT that has moved away from the traditional compliance approach and being much more about learning and evolving for both supervisors and supervised entities.

TIBER-EU framework benefits as seen by service providers	Ensuring a level playing field and a benchmark across the different financial services players in Malta and within the EU.
	Learning from TIBER assessment results and evolving to the next level of cyber resilience by implementing the remediation plan based on the assessment's findings.
	Allowing cross-jurisdictional cooperation between authorities, preventing pan-European financial entities from being tested several times.
	Maximising the test learning experience by using the so-called "leg-ups" (the assistance or information provided by the white team to the testers to allow the testers to continue the execution of an attack path where they are not able to advance on their own, including for insufficient time or resources in a given TLPT).
	Involving the national TCT, with the aid of the TKC, that facilitates communication and a good flow of information between all involved parties at the appropriate time during the entire test process.
	Due to the involvement of regulatory authorities, board level involvement tends to be higher than in other tests carried out by entities.
	Improving the relationship and collaboration between entities in the financial sector by learning not only from their own tests, but from all tests carried out in the sector.
	Allocating cybersecurity resources more effectively by identifying areas of improvement that are currently the target of real threat actors.
	Harmonisation in the regulatory landscape of entities with a presence in multiple jurisdictions, saving resources and costs for both the regulator and financial entities.

Figure 7: TIBER-EU framework benefits as seen by service providers

3.2.3 TIBER-EU risks and challenges as seen by service providers

A number of difficulties are envisaged by service providers.

More complexity, a longer period of testing and more expensive than a standard penetration test.	Managing more actors and a larger variety of stakeholders involved and internal resources needed at the entity level for managing the assessment.	Requires to be delivered by senior individuals, needs the active involvement from the customer and normally targets the most critical functions of entities.
Managing inherent risks, such as denial of service, temporary loss of services, unexpected system crashes, unwanted disruption, damage to critical live production systems, loss/modification/disclosure of sensitive data, and a real attack occurring during the test.	Stressful experience for personnel being targeted in phishing attacks and privacy concerns related to the personal data acquired.	Implementing appropriate controls, processes and procedures to ensure that the test is carried out with sufficient assurances for all stakeholders, that risks will be identified, analysed and mitigated according to best practices in risk management.
For a useful test outcome, the entities should be fully open and collaborate with service providers and authorities, the assessment itself being a learning exercise not a pass or fail test.	Dealing with test plan deviations during the test execution and/or recognising the circumstances that could lead to a transition to a purple teaming exercise instead of continuing with red teaming.	Recognising a strong security posture of the tested entity when the test objectives seem unachievable.
The outcome of the test is highly dependent on the quality of Threat Intelligence (TI) and Red Team (RT) providers.	Challenging procurement for external TI and RT providers, especially in smaller markets.	Although TIBER is an end-to-end test with multiple scenarios, it will not identify every single weakness in the cyber resilience of the entity.

Figure 8: TIBER-EU risks and challenges as seen by service providers

3.3 Industry Views on the Introduction of TIBER-EU in Malta

This sub-section addresses questions Q3.1 to Q3.3 of the Consultation Document, in which the Authority asked about industry views in relation to the introduction of a TIBER-EU framework in Malta (TIBER-MT) and the benefits, risks, opportunities, and challenges foreseen.

3.3.1 Financial entities' views on the introduction of the TIBER-EU framework in Malta

All Financial Entities consider that the introduction of the framework locally would be beneficial for the financial services sector. Specific reference was made to the banking sector where such framework is viewed to increase the resilience. Consequently, the framework is seen to increase consumer protection.

Financial entities' foreseen risks and challenges related to the introduction of the TIBER-EU framework in Malta	Cost of tests.
	Resources/skills necessary to manage the tests.
	Lack of threat intelligence pertaining to the financial institutions in Malta.
	Necessary considerations for multinational organisations and the multi-jurisdictional approach for these tests.

Figure 9: Financial entities' foreseen risks and challenges related to the introduction of TIBER-EU in Malta

3.3.2 Service providers' views on the introduction of the TIBER-EU framework in Malta

The introduction of the TIBER-EU framework in Malta is seen as a very good opportunity to increase the cyber resilience of Maltese financial entities and thus contributing to financial stability. Also, this approach would bring more confidence in the financial sector for customers, investors, counterparties, and other stakeholders.

A TIBER-MT framework could bring Malta's core financial entities together in a cyber information and intelligence sharing initiative contributing to the resilience of the wider financial sector ecosystem. The TIBER-EU framework could be adopted to suit the needs of a smaller market size ensuring that Malta as a financial services hub does not lose its competitive advantage in the future. TLPTs would close potential gaps between the security posture level of the local financial sector and that of other larger member states who have already adopted the framework.

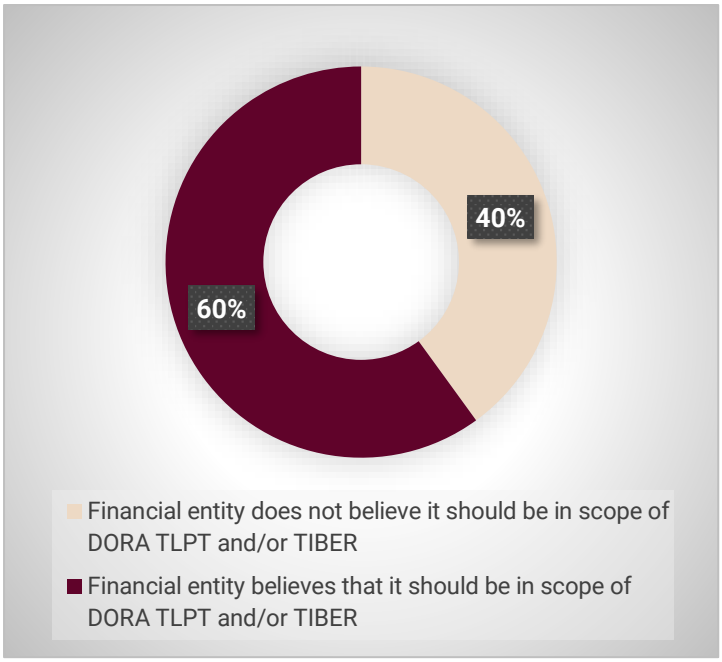
Taking in consideration that DORA has entered into force as of January 2023 and will fully apply from January 2025, the adoption of TIBER-MT could provide the competent authorities and core financial entities with the needed relevant knowledge and experience.

3.4 Entities in Scope of Advanced Testing Based on TLPT/TIBER-EU

This sub-section addresses questions Q3.4, Q4.1, Q4.2, and Q5.1 of the Consultation Document, in which the Authority asked about the financial entities that should fall within scope of advanced testing based on TLPT and/or the TIBER-EU framework. The consultation further explored the aptitude of financial entities towards conducting such testing on a voluntary basis (outside a mandatory obligation).

3.4.1 Financial entities' views on entities in scope of advanced testing based on TLPT and/or the TIBER-EU framework

The banking sector is widely regarded as the most important sector that should be included within the scope of advanced testing based on TLPT and/or the TIBER-EU framework. References were also made to financial entities with a direct and meaningful impact on the overall financial system. Sectors of high criticality (as annexed within NIS2[6]) are also seen as good candidates.



The entities considered to be in scope of advanced testing based on TLPT (DORA) and/or the TIBER-EU framework see regular resilience testing as an essential component of maintaining their cyber-security.

The entities that do not believe they should be in scope due to size and importance, consider other tools to increase operational resilience (e.g. penetration tests). They do not rule out undertaking TLPT/TIBER on a voluntary basis or plan to incorporate elements of TLPT/TIBER in their

Figure 10: Financial entities' views on whether they should be in scope of advanced testing based on TLPT and/or TIBER-EU (financial entities' views)

[6] DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)

3.4.2 Service providers' views on entities in scope of advanced testing based on TLPT and/or the TIBER-EU framework

Service providers see the TIBER-EU framework especially suited for entities that play a key role in the financial system and should only be applied to financial entities which are relatively "cyber mature", having already implemented proper cyber risk controls in place. Service providers mentioned that the framework should be recommended to entities in the financial sector and compulsory to those organisations which support the country in mission critical functions.

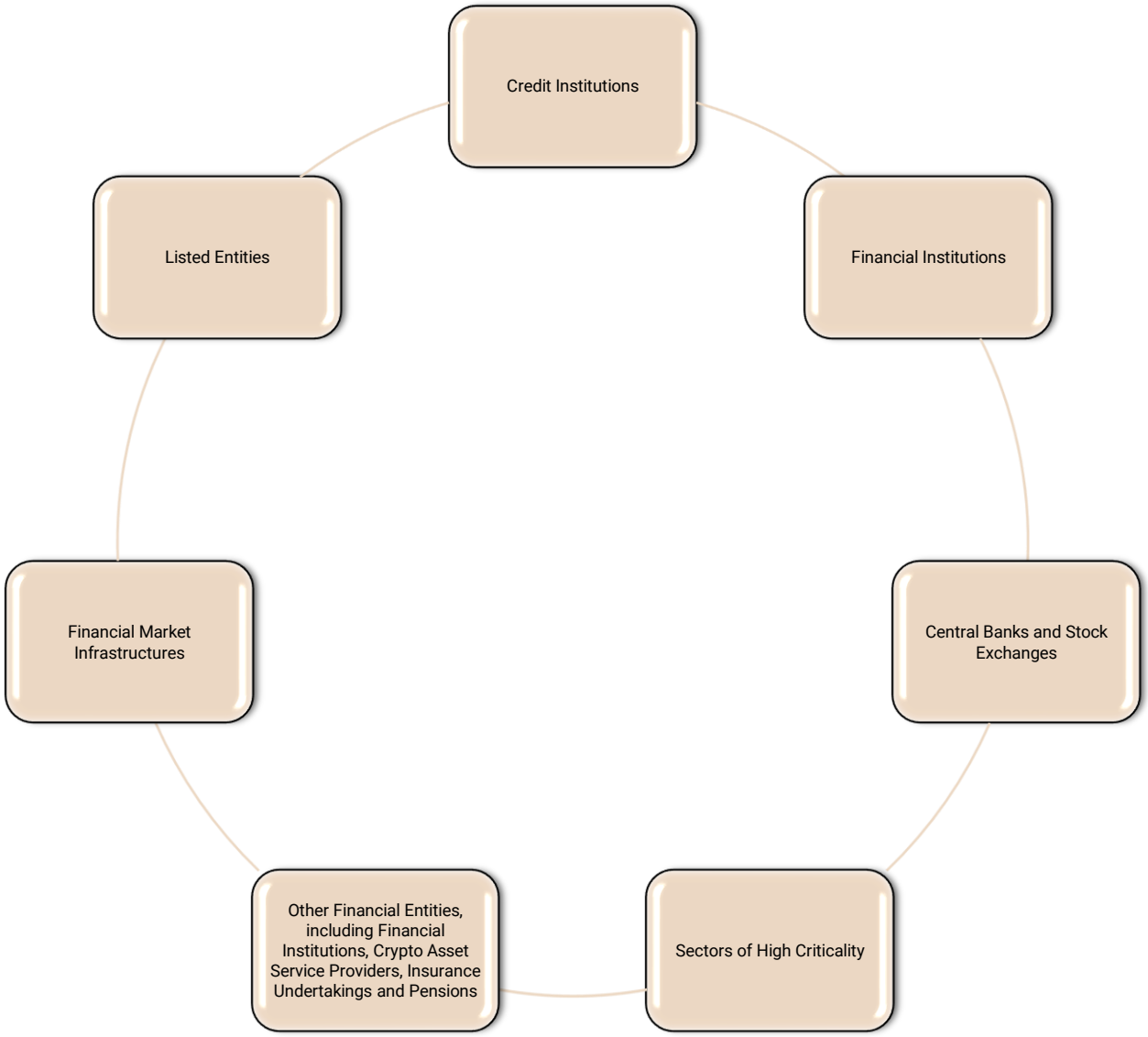
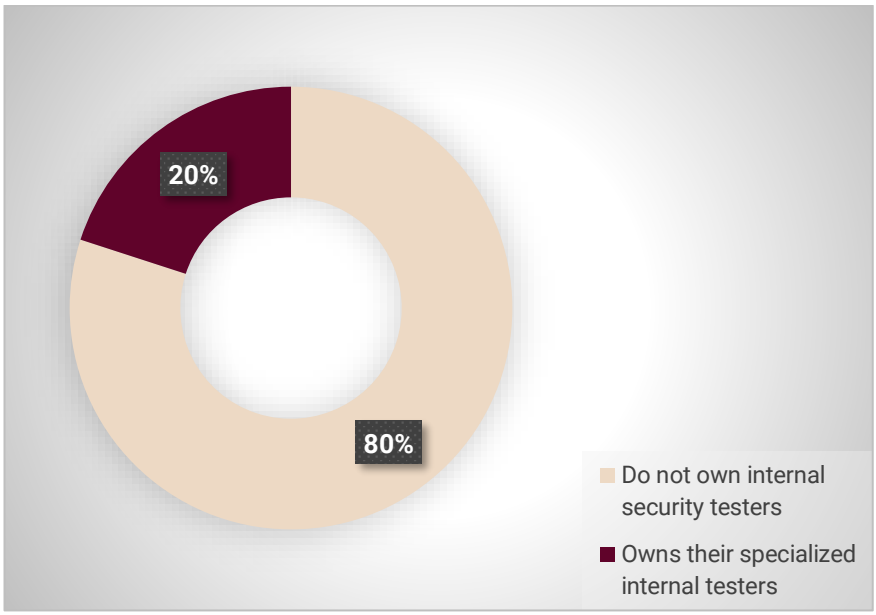


Figure 11: Entities in scope of advanced testing based on TLPT and/or TIBER-EU (service providers' views)

3.5 Internal Testers

This sub-section addresses questions Q4.3 and Q5.2 of the Consultation Document, in which the Authority asked about internal testers within financial entities with the necessary knowledge and skills that could potentially participate in advanced testing based on TLPT and/or the TIBER-EU framework.



The majority of responding financial entities consider the use of external testers for their testing activities. Some financial entities also consider investing in additional information security personnel with the necessary knowledge to assist and review test reports from external third parties.

Figure 12: Internal testers within financial entities

3.6 Internal Capabilities Required by Financial Entities

This sub-section addresses questions Q6.1 to Q6.3 of the Consultation Document, in which the Authority asked about the necessary resources and skills needed by financial entities for conducting and managing advanced testing based on TLPT and/or the TIBER-EU framework.

Given the specialised nature of the activities required to be undertaken during a TLPT/TIBER-EU test, only a very small part of the respondents mentioned that the existing internal resources and skills are sufficient for managing these kinds of tests. However, all the entities are aware that specialised training would result in better preparation and carrying out proper test management.

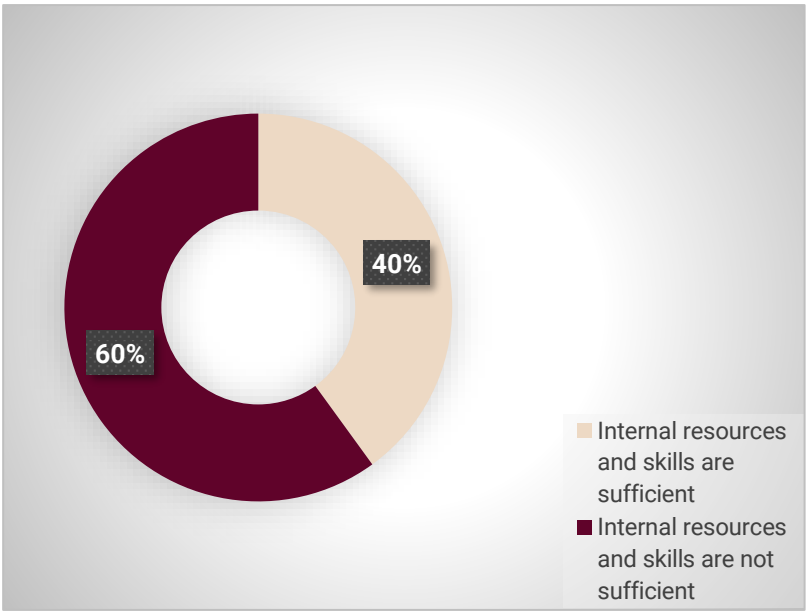


Figure 13: Internal capabilities required by financial entities

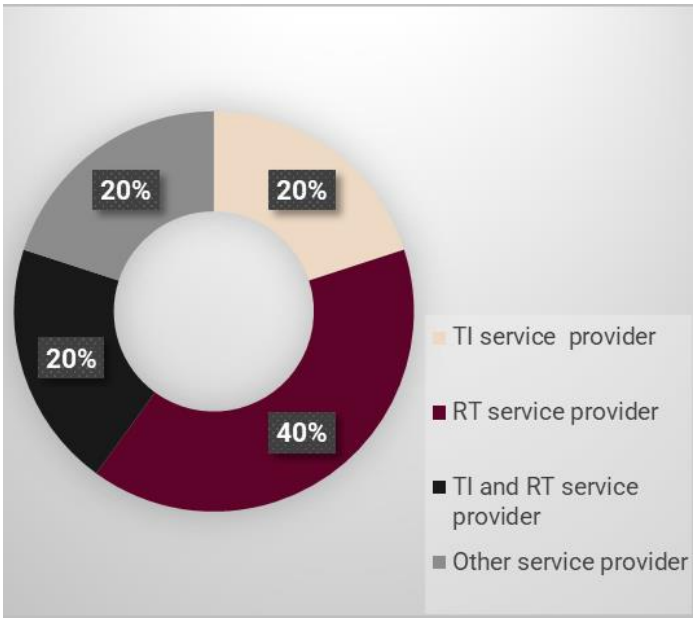
Financial entities foresee additional training for their internal teams to enhance their knowledge and skillset.

Training foreseen by financial entities	Introduction to the TIBER-EU framework.
	More specific, in-depth TIBER-EU trainings.
	Specialised training from a White Team perspective.

Figure 14: Training foreseen by financial entities

3.7 Providing Threat Intelligence and/or Red Team Services

This sub-section addresses questions Q7.1 and Q7.2 of the Consultation Document, in which the Authority asked about the capabilities of the service providers to offer Threat Intelligence and/or Red Team services to the local financial sector, at entity level or in partnership with other service providers.



The Authority has garnered responses from a variety of service providers. This chart depicts their distribution based on the services that they provide.

Furthermore, all responding Threat Intelligence and/or Red Team service providers mentioned that they already provide or consider providing services for advanced testing based on TLPT (DORA) and/or the TIBER-EU framework.

Figure 15: Providing Threat Intelligence and/or Red Team services

3.8 Participation in Industry Fora, Groups and Cooperation Networks

This sub-section addresses Q8.1 to Q8.5 of the Consultation Document, in which the Authority asked about the respondents' experience and aptitude to participate in industry fora, groups and cooperation networks.

3.8.1 Financial entities' views on industry cooperation

All responding financial entities showed interest in participating in industry fora, groups, and cooperation networks.

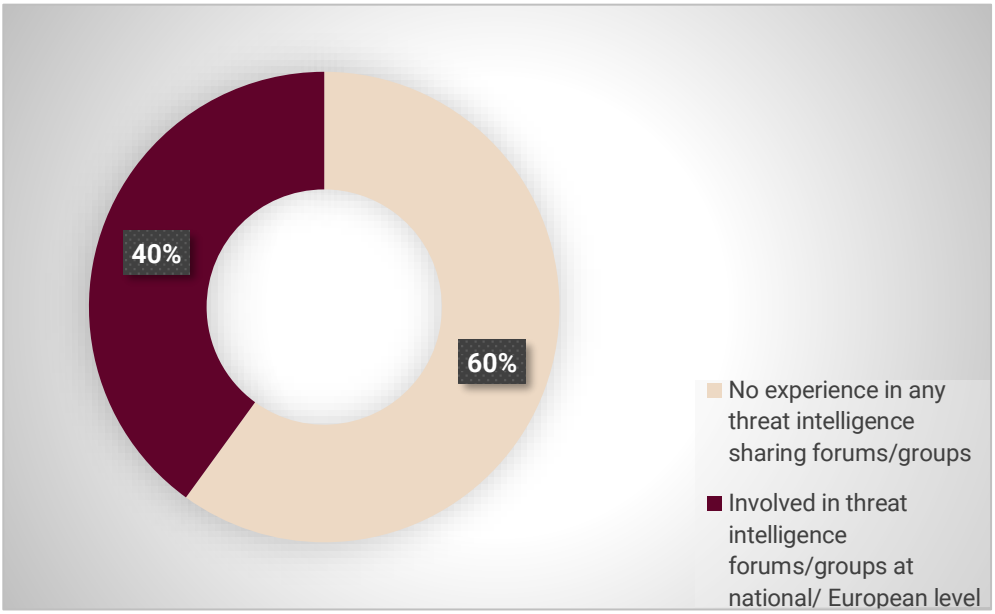


Figure 16: Participation in industry fora, groups and cooperation networks

Lessons learnt from participation in industry fora, groups and networks	The bigger the group, the less likely participants would share information.
	Ad hoc participants would be welcome, based on the topic discussed.
	In person meetings are preferred (at least in the beginning) to build trust.
	Most groups depend on few frontrunners to get started.
	The role of joiners from regulators/authorities has to be understood by all participants otherwise they will be hesitant to share.

Figure 17: Lessons learnt from participation in industry fora, groups, and cooperation networks

One respondent expressed a view that even though a lot of valuable information is shared through industry fora, in many cases communication flows are ineffective, mentioning that direct relationships with other financial entities could add more value in this regard.

3.8.2 Service providers' views on industry cooperation

Most of the respondents are involved in threat intelligence sharing groups, including some cyber information and intelligence sharing initiatives across the EU, such as the Cyber Information and Intelligence Sharing Initiative (CIISI-EU[7]). Sharing information, intelligence, and good practices, and raising awareness of cybersecurity threats is considered an effective method of improving the capabilities of the financial sector to prevent, detect, and respond to cyberattacks.

All responding service providers expressed interest in participating within cooperation networks but stressed that competent authorities should act as catalysts in setting-up such initiatives at a national level, building the necessary trust among the participants.

The implementation of the TIBER-EU framework will not only increase the cyber resilience of the entities that undergo the tests, but it will also foster cooperation and sharing of best practices and therefore lead to increased cyber resilience in the sector as a whole.

[7] https://www.ecb.europa.eu/press/pr/date/2020/html/ecb.pr200227_1~062992656b.en.html

3.9 Other Feedback

This sub-section addresses Q9 of the Consultation Document, in which the Authority asked about any other feedback from respondents.

The Authority received feedback in relation to ring-fencing, currently in place in typical TIBER-EU framework implementations, between the function (within an authority) responsible for overseeing TIBER tests and the function carrying out ongoing supervisory activities. The respondent explained that with DORA, TIBER-EU may become a regulatory tool and therefore the relationship between the TIBER Cyber Team and the financial entity might change. This could potentially lead to entities not doing more than is required by the framework and in so doing they would miss potential learning outcomes.

Other feedback	In many countries, initiatives driven by financial regulators have then been followed by other industries. This initiative is seen as an important step forward for the security in Malta.
	Most of the authorities that adopted the TIBER-EU framework produce a GTL (usually outsourced to an external threat intelligence provider) for the benefit of all entities that will undergo TIBER tests, because the strategic overview of the threat landscape overlapped significantly for most entities.
	A pilot is recommended comprising the most cyber mature organisations and/or entities that already did red teaming exercises.
	The TIBER-EU framework is generic enough to work in every country and it allows for specific changes to be made for every implementation.

Figure 18: Other feedback

3.10 MFSA Feedback to Queries from the Industry

No.	Question	MFSA response
1.	Is the local implementation of TIBER-EU foreseen to introduce major changes to the framework to suit the local market particularities?	The implementation of the TIBER-EU framework must be in accordance with the mandatory requirements of the TIBER-EU framework and optional requirements at the jurisdiction's discretion.
2.	Will there be accreditation for the providers delivering TI/RT services?	As at the date of this document, the Authority is not aware of any TIBER-EU accreditation providers in the EU, nor is the Authority aware of any accreditation providers in the pipeline. The Authority will be in a position to provide further clarity on this aspect at a later stage.
3.	Will the establishment of TIBER-MT be ultra vires, complementary or substitutionary to the provisions of DORA (with DORA being aligned with TIBER 2.0), in particular the provisions of RTS/ITS issued thereunder?	The implementation of the TIBER-EU framework must be in accordance with the mandatory requirements of the TIBER-EU framework. A revision of the current TIBER-EU framework, aligned with the respective DORA Regulatory Technical Standard (still under public consultation as at the date of this document) is expected to be released in due course. As the DORA TLPT Regulatory Technical Standards are being developed "in accordance with TIBER-EU", the completion of a TIBER-EU test should satisfy the required DORA TLPT provisions.
4.	Which public authority shall be designated in line with the provisions of Article 26(9) or 26(10) DORA? under TIBER-EU (Section 3.7). What role will the MFSA play in the context of the TIBER-MT?	Please refer to the Consultation Document on the National Implementation of Regulation (EU) 2022/2554 and Transposition of Directive (EU) 2022/2556 on Digital Operational Resilience for the Financial Sector. As part of the implementation of the TIBER-EU framework, such information is made available in the TIBER-XX Guide.
5.	Some guidance from the designated authority on the Code Names (Section 6.8) and reporting of findings for anonymity purposes?	Due to the sensitivity of the tests, an entity being tested, within the context of the test (for instance within documentation and communication), is referred to by an agreed code name rather than by explicitly naming the entity.

6.	What would be the communication channel for TIBER-MT? Would information obtained in relation to and during TIBER-MT test be channelled through an EU system? If so, which one?	Communication channels are determined by the financial entity being tested. Any required communications with the European Central Bank (for instance, as the competent authority for credit institutions classified as significant in accordance with Article 6(4) of Regulation (EU) No 1024/2013) will use communication channels established by the European Central Bank.
7.	Will TIBER-MT require introduction of specific contractual clauses into the contracts entered into with the testers/overall TPPs and outsourcing service providers?	The implementation of the TIBER-EU framework must be in accordance with the mandatory requirements of the TIBER-EU framework.
8.	Can the MFSA confirm whether Article 26(8) second subparagraph.: "Credit institutions that are classified as significant in accordance with Article 6(4) of Regulation (EU) No 1024/2013, shall only use external testers in accordance with Article 27(1), points (a) to (e)." shall be understood as such external testers shall not be considered as outsourced service providers but shall be excluded from the scope of outsourcing in line with para. 28(a) of the EBA Guidelines on outsourcing arrangements stating: "28. As a general principle, institutions and payment institutions should not consider the following as outsourcing: (a) a function that is legally required to be performed by a service provider, e.g., statutory audit"?	This question goes beyond the objective of this public consultation which was not issued to reflect upon the definition of outsourcing and/or what should or should not be considered as outsourcing.

9.	Will the designated authority appoint its own security partners to provide a generic assessment on the national financial sector threat landscape so entities can use it as a guideline? Has the MFSA evaluated the possibility of producing a localised GTL report that would be made available to the parties in-scope of TLPT?	A Generic Threat Landscape Report is an optional requirement under the TIBER-EU framework and is being taken into consideration. The production of any such report will be communicated accordingly.
10.	What will the process be if the designated authority considers that the conduct of test was not in line with requirements and spirit of TIBER-MT. Will it be reconsidered vis-à-vis TIBER-EU/ DORA requirements?	Each case will need to be assessed and acted upon according to its own merit and in accordance with the applicable frameworks and/or regulatory provisions.
11.	Does TIBER-MT foresee validation and/or approval of providers to conduct TLPT at the entity's level? Does the MFSA foresee to issue such validation/approval of testers also under DORA regime?	The implementation of the TIBER-EU framework must be in accordance with the mandatory requirements of the TIBER-EU framework. The respective DORA Regulatory Technical Standard (still under public consultation as at the date of this document) provides that "The TLPT authority may object to the selected threat intelligence providers and external testers where they do not ensure compliance with Article 5(2) or national security legislations".

12.	**[1]** Would the entity need to get approval/set checkpoint meetings with the designated authority/team on the process/goals. **[2]** To this end, would generic guidelines be issued by the designated authority on what needs to be tested/covered? **[3]** What would be the interplay between such guidelines under TIBER-MT and DORA Level 2 Laws?	**[1]** Recital 12 of the respective DORA Regulatory Technical Standard (still under public consultation as at the date of this document) provides that "As evidenced by the experience of the implementations of the TIBER-EU framework, holding in-person or virtual meetings including all relevant stakeholders (financial entity, authorities, testers and threat intelligence providers) is the most efficient way to ensure the appropriate conduct of the test. Therefore in-person and virtual meetings are strongly encouraged and should be held at various steps of the process, and in particular: during the preparation phase at the launch of the TLPT and to finalise on its scope; during the testing phase, to finalise the threat intelligence report and the red team test plan and for the weekly updates; and during the closure phase, for the purposes of replaying testers and blue team actions, purple teaming and to exchange feedback on the TLPT". **[2]** Under the TIBER-EU framework the scope must include the entity's critical functions. Art.26(2) subpara.3 of DORA stipulates that "Financial entities shall assess which critical or important functions need to be covered by the TLPT. The result of this assessment shall determine the precise scope of TLPT and shall be validated by the competent authorities." Furthermore, the criteria to be considered for the inclusion of critical or important functions in the scope of the TLPT are provided within the respective DORA Regulatory Technical Standard. **[3]** A revision of the current TIBER-EU framework, aligned with the respective DORA Regulatory Technical Standard is expected to be released in due course.
13.	How will the entities be selected for participating in TIBER-MT tests and what guidance will be provided to these organisations?	The selection of the entities is expected to follow the respective DORA Regulatory Technical Standard (still under public consultation as at the date of this document). As part of the implementation of the TIBER-EU framework, guidance is made available in the TIBER-XX Guide.

14.	What is the approach for multi-jurisdictional entities?	The approach for entities operating in more than one Member State is expected to follow the respective DORA Regulatory Technical Standard (still under public consultation as at the date of this document).
15.	Should TIBER-MT go beyond the applicability of DORA, potentially the home-grown types of entities (e.g., Trustees and CSP) could be included?	The selection of the entities is expected to follow the respective DORA Regulatory Technical Standard (still under public consultation as at the date of this document).
16.	The TIBER will remain a framework to adopt and follow or if it will become certifiable with a certificate of attestation like PCI DSS is for example?	The TIBER-EU framework and DORA provide for attestation rather than certification.
17.	In most countries which have implemented the TIBER-EU framework at national level, it is the national central bank, in a catalyst, non-supervisory role, which takes the lead. What are the responsibilities of the MFSA and the Central Bank of Malta in this context?	Please refer to the Consultation Document on the National Implementation of Regulation (EU) 2022/2554 and Transposition of Directive (EU) 2022/2556 on Digital Operational Resilience for the Financial Sector. As part of the implementation of the TIBER-EU framework, such information is made available in the TIBER-XX Guide.

18.	**[1]** How are the best ways to align with DORA's requirements in TLPT area provided that the RTS on this topic will be available in late 2024? **[2]** TIBER-based TLPT performed in 2023 and 2024 would comply with DORA requirements regardless of the outcome from the RTS? **[3]** Which type of entities would fall in scope of TLPT under DORA, as well as by when such entities would be expected to have undergone a TLPT in view of the 17 January 2025 day of applicability of the DORA regulation?	**[1]** This is a shared challenge for all stakeholders. The respective DORA Regulatory Technical Standard (still under public consultation as at the date of this document) provides that "The financial entity shall submit the initiation documents to the TLPT authority within three months from having received a notification from the TLPT authority that a TLPT shall be carried out" and "The scope specification document shall…be submitted to the TLPT authority within six months from the receipt of the notification from the TLPT authority". **[2]** Recognised TLPTs are planned to commence after the date of applicability of DORA. **[3]** Please refer to the response provided for Questions 13 and 15 and the lead times quoted for Question 18 [1].

References

Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector.

ECB (2018) TIBER-EU framework. How to implement the European framework for Threat Intelligence-based Ethical Red Teaming. Available at: https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf (Accessed: January 2024).

ECB (2018) TIBER-EU framework. Services Procurement Guidelines. Available at: https://www.ecb.europa.eu/pub/pdf/ecb.tiber_eu_services_procurement_guidelines.en.pdf (Accessed: January 2024).

ECB (Various) TIBER-EU framework. Available at: https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html (Accessed: January 2024).

Annex A: Consultation Questions

Q1 **[A, B, C, D]***	**Q1.1** Do you have any experience in the field of Threat-Led Penetration Testing within your organisation?
	Q1.2 If yes, can you share your experience?
	Q1.3 If yes, how close to the TIBER-EU framework and/or the provisions of DORA was this testing?
	Q1.4 If yes, can you share any information in relation to the benefits, risks, opportunities or challenges encountered and any lessons learnt?
Q2 **[A, B, C, D]***	**Q2.1** Do you have any experience in any aspect of the TIBER-EU framework within your organisation?
	Q2.2 If yes, can you share your experience?
	Q2.3 If yes, can you share any information in relation to the benefits, risks, opportunities or challenges encountered and any lessons learnt?
Q3 **[A, B, C, D]***	**Q3.1** What are your views in relation to the introduction of a TIBER-EU framework in Malta (TIBER-MT)?
	Q3.2 What queries or areas of clarification do you have on the matter?
	Q3.3 What benefits, risks, opportunities and challenges do you foresee for your organisation and for industry stakeholders in Malta?
	Q3.4 Which entities do you believe should be included within scope?
Q4 **[A]***	**Q4.1** Do you believe that your entity should fall within the scope of, and thus be required by law to conduct, advanced testing based on TLPT as provided by DORA and/or the TIBER-EU framework[8] every three (3) years?
	Q4.2 If yes, what benefits, risks, opportunities and challenges do you foresee for your organisation?
	Q4.3 If yes, does your organisation have internal testers (including within the group if applicable) with the necessary knowledge and skills that could potentially participate in such tests? In the absence of the RTS and any accreditation/certification framework, please be guided by Sections 3 and 4 of the TIBER-EU Framework Services Procurement Guidelines.
Q5 **[A]***	**Q5.1** If you do not believe that your entity should fall within the scope of, and thus be required by law to conduct, advanced testing based on TLPT as provided by DORA and/or the TIBER-EU framework, would you consider undertaking TLPT and/or TIBER on a voluntary basis?

[8] The local relevant authorities will provide a timeframe for TIBER tests for entities that are required to perform these tests.

Q5 **[A]***	**Q5.2** Does your organisation have internal testers (including within the group if applicable) with the necessary knowledge and skills that could potentially participate in such tests? In the absence of the RTS and any accreditation/certification framework, please be guided by Sections 3 and 4 of the TIBER-EU Framework Services Procurement Guidelines.
Q6 **[A]***	**Q6.1** In the case of a TLPT/TIBER test, do you think that your entity has the necessary internal resources and skills (from a financial entity perspective) for the test to be conducted in accordance with the requirements outlined in the TIBER-EU White Team Guidance or do you need to seek additional resources (through hiring and/or outsourcing)?
	Q6.2 In addition to the general guidance on the TLPT/TIBER tests and the specific support that will be provided by National Competent Authorities for each test, do you think that more specialised training is necessary for the team within your entity for better preparation and proper test management?
	Q6.3 What types of training resources might you consider?
Q7 **[B]***	**Q7.1** Is your organisation providing and/or considering/planning to provide any of the services?
	Q7.2 Do you think that your organisation can potentially provide any of the TLPT/TIBER services alone or in association with other service providers? In the absence of the RTS and any accreditation/certification framework, please be guided by Sections 3 and 4 of the TIBER-EU Framework Services Procurement Guidelines.
Q8 **[A, B, C, D]***	**Q8.1** Do you have experience in participating in any industry forums/groups for threat intelligence sharing?
	Q8.2 If yes, can you share your experience?
	Q8.3 If yes, can you share any information in relation to the benefits, risks, opportunities or challenges encountered and any lessons learnt?
	Q8.4 Would you be interested in participating in any working groups on TLPT as provided by DORA and/or the implementation of the TIBER-EU framework in Malta?
	Q8.5 Following the implementation of DORA and the TIBER-EU framework, do you consider it would be useful to participate in a financial industry cooperation network (led by competent authorities) to share the experience gained from the tests?
Q9 **[A, B, C, D]***	**Q9** Do you have any other feedback?

* Note letter references below:

[A] Financial entities interested in undertaking TIBER-EU tests.
[B] Organisations interested in providing cyber threat intelligence/red teaming testing services under the TIBER-EU framework.
[C] National intelligence agencies and relevant government departments.
[D] Any other interested party.