MFSA MALTA FINANCIAL SERVICES AUTHORITY

Consultation Document

Consultation on the Adoption of the TIBER-EU Framework in Malta

Ref: 03-2023

Date: 08 March 2023

Closing Date: 06 April 2023

NOTE: This document is circulated by the MFSA for the purpose of consultation of industry stakeholders. Accordingly, no decision on how, when and by whom the framework under this consultation will be implemented in Malta was taken. It is important that entities involved in the consultation bear these considerations in mind.

Contents

Triq l-Imdina, Zone 1 Central Business District, Birkirkara CBD 1010
+356 2144 1155

communications@mfsa.mt
www.mfsa.mt

1. Executive Summary

This consultation document is being issued to firstly introduce the TIBER-EU (**T**hreat **I**ntelligence-**B**ased **E**thical **R**ed-Teaming) framework to interested industry stakeholders as well as the relationship between its requirements and the requirements of the Digital Operational Resilience Act (hereinafter referred to as DORA) on advanced testing based on threat-led penetration testing (TLPT). Secondly, this consultation seeks to gather the views of industry stakeholders on the adoption of the TIBER-EU framework in Malta.

2. Introduction

In May 2018, the European Central Bank published the TIBER-EU framework[1], the first EU-wide framework for threat intelligence-based ethical red-teaming that provides 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 form the core European financial infrastructure to test and enhance their protection, detection, and response capabilities.

TIBER-EU was designed to be adopted by relevant authorities in any jurisdiction, on a voluntary basis. The framework is currently implemented, or being implemented, in Belgium, Denmark, Finland, Germany, Ireland, Italy, Norway, Portugal, Romania, Spain, Luxembourg, Sweden, and the Netherlands, as well as by the ECB in its oversight capacity.

The TIBER-EU framework specifies that certain criteria should be followed when carrying out advanced testing. Testing should be carried out on the entity's live production environment, targeting its critical functions. Such testing is to be conducted by independent, highly skilled, third-party providers (the thread intelligence team and the red teaming team). The test needs to be performed without the knowledge of the target entity's security/response capability and only a small group (white team) in the entity would know about it, which is to be responsible, together with the management, of the overall test on the part of the entity. The test will not result in a pass or fail but will enable the entity to learn and evolve to a higher level of cyber maturity.

[1] The framework is complemented with the following supporting documents issued by the ECB: TIBER-EU Services Procurement Guidelines, TIBER-EU White Team Guidance, TIBER-EU Attestation template, TIBER-EU Guidance for Target Threat Intelligence Report, TIBER-EU Guidance for the Red Team Test Plan, TIBER-EU Scope Specification Template, TIBER-EU Guidance for the Red Team Test Report, TIBER-EU Guidance for Test Summary Report, and TIBER-EU Purple Teaming Best Practices.

Triq l-Imdina, Zone 1 Central Business District, Birkirkara CBD 1010
+356 2144 1155
communications@mfsa.mt
www.mfsa.mt

3. Current Situation

DORA Advanced Testing and TIBER-EU Framework

On 27 December 2022, Regulation (EU) 2022/2554 and Amending Directive (EU) 2022/2556 on Digital Operational Resilience for the Financial Sector (DORA) were published on the Official Journal of the European Union (EU) and entered into force on 16 January 2023[2].

DORA aims to increase the digital operational resilience of financial entities within scope and introduces requirements for financial entities, identified by National Competent Authorities based on their significance, to conduct advanced testing based on TLPT.

The European Supervisory Authorities are to develop Regulatory Technical Standards (RTS) regarding advanced testing based on TLPT in accordance with the TIBER-EU framework[3] and submit the RTS to the European Commission by 17 July 2024. In this regard, the TIBER-EU framework and the RTS are required to be aligned.

The Adoption of TIBER-EU in Malta

The relevant authorities which would be responsible for adopting and implementing TIBER-EU in Malta need to consider which entities could be invited to participate in the test, based on the intended purpose of the national implementation (as a supervisory or oversight tool, for financial stability purposes, or as a catalyst).

Article 26(8) of DORA states that competent authorities are to identify financial entities required to perform TLPT based on an assessment of impact-related factors, possible financial stability concerns and specific ICT risk profile / level of ICT maturity of the financial entity or technology features involved.

The Malta Financial Services Authority (MFSA) is currently working on the adoption and implementation of the TIBER-EU framework in Malta, within the context of the DORA implementation by 17 January 2025.

[2] On 4 January 2023, the MFSA published a circular in this regard.
[3] As specified in Article 26(11) of DORA.

Triq l-Imdina, Zone 1 Central Business District, Birkirkara CBD 1010
+356 2144 1155
communications@mfsa.mt
www.mfsa.mt

4. Consultation Feedback

This consultation is intended to all industry stakeholders interested in the adoption and implementation of the TIBER-EU framework in Malta, including:

- financial entities[4] interested in undertaking TIBER-EU tests
- organisations interested in providing cyber threat intelligence/red teaming testing services under the TIBER-EU framework
- national intelligence agencies and relevant government departments, and
- any other interested party.

Annex A provides a structure to the consultation by outlining a number of questions. Industry stakeholders are encouraged to provide any other feedback which is not necessarily addressed by the outlined questions.

5. Way Forward

MFSA is seeking feedback from relevant stakeholders prior to proceeding with the adoption and implementation of the TIBER-EU framework. Industry stakeholders are invited to submit their feedback by sending an email to sirc@mfsa.mt at the earliest and by not later than 6 April 2023. Respondents should identify themselves and the organisation (if applicable) they represent. Participating organisations should send one set of feedback per organisation or per group (if/where applicable). Financial entities may choose to send a consolidated set of feedback through their association.

[4] Financial entities in scope of TIBER-EU framework are payment systems, central securities depositories, central counterparty clearing houses, trade repositories, credit rating agencies, stock exchanges, securities settlement platforms, banks, payment institutions, insurance companies, asset management companies and any other service providers deemed critical for the functioning of the financial sector.

Triq l-Imdina, Zone 1 Central Business District, Birkirkara CBD 1010
+356 2144 1155
communications@mfsa.mt
www.mfsa.mt

Annex A

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[5] 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?

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

Triq l-Imdina, Zone 1 Central Business District, Birkirkara CBD 1010
+356 2144 1155
communications@mfsa.mt
www.mfsa.mt

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.

Triq l-Imdina, Zone 1 Central Business District, Birkirkara CBD 1010
+356 2144 1155
communications@mfsa.mt
www.mfsa.mt