MFSA MALTA FINANCIAL SERVICES AUTHORITY

Comparing the TIBER-EU Framework with Other Established Non-EU TLPT Frameworks

A mapping exercise comparing the TIBER-EU framework with other Threat-Led Penetration Testing Frameworks established outside of the European Union, namely CBEST, iCAST, AASE, and I-CRT.

CONTENTS

REVISIONS LOG

VERSION	DATE ISSUED	DETAILS
1.00	16/06/2026	Document Issued

1. Introduction

1.1. Background

As of 18 June 2025, Commission Delegated Regulation (EU) 2025/1190 ('RTS on TLPT')[1] supplementing Regulation (EU) 2022/2554 (the 'DORA Regulation')[2] entered into force. This requires that financial entities ('FEs') falling within the scope of Article 26(1) of the DORA Regulation and assessed pursuant to Article 2(1) or 2(2) of the RTS on TLPT to conduct threat-led penetration testing ('TLPT').

For the purpose of conducting a TLPT engagement, FEs are required to select TLPT providers, including threat intelligence providers and external or internal testers, in accordance with Article 7 of the RTS on TLPT, see **Annex I**. Certain requirements under Article 7 of the RTS on TLPT, see **Annex I**, refer to previous assignments relating to penetration testing and red team testing activities. Given the relatively recent introduction of mandatory TLPT exercises under the DORA Regulation, the availability of previous assignments conducted specifically as TLPT engagements may be limited. This may affect the fulfilment of Article 9(1) of the RTS on TLPT, for both FEs when selecting TLPT providers and competent authorities when assessing whether the providers proposed by an FE meet the applicable requirements.

However, the European Securities and Markets Authority ('ESMA'), in its Final Report[3] submitted on 17 July 2024, further noted in Chapter 1, paragraph 4, that:

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

Furthermore, the Bank of Italy, in a paper published on May 2026[4] on the Italian market for cybersecurity testing services, identified a shortage of skilled professionals and market concentration as relevant indicators of limited provider depth within the TLPT sector.

1.2. Scope

In February 2025, the European Central Bank ('ECB') updated their framework on threat intelligence-based ethical red-teaming ('TIBER-EU framework')[5] to fully align it with the RTS on TLPT supplementing the DORA Regulation. The TIBER-EU framework ensures

[1] Delegated regulation - EU - 2025/1190 - EN - EUR-Lex
[2] Regulation - 2022/2554 - EN - DORA - EUR-Lex
[3] JC 2024-29 - Final report on DORA RTS on TLPT
[4] Exploratory Survey of the Italian Market for Cybersecurity Testing Services by Anna Barcheri, Luca Bastianelli, Tommaso Curcio, Luca De Angelis, Paolo De Joannon, Gianluca Ralli, Diego Ruggeri :: SSRN
[5] "TIBER-EU framework How to implement the European framework for Threat Intelligence-Based Ethical Red teaming"

a qualitative, controlled, and safe TLPT approach across the EU. It provides comprehensive guidance for cyber resilience testing and facilitates a uniform and harmonised approach for TLPT for FEs across Europe.

Voluntary TIBER tests have been conducted within the European Union since May 2018. Accordingly, previous experience obtained through TIBER tests may be relevant when assessing compliance with Article 7 of the RTS on TLPT, see **Annex I**.

However, market participants may also have obtained relevant practical experience through established non-EU threat intelligence-led testing frameworks. This document therefore assesses recognised non-EU frameworks, namely CBEST, iCAST, AASE, and I-CRT, to determine whether experience obtained under such frameworks may support the assessment of TLPT provider requirements under Article 7 of the RTS on TLPT, see **Annex I**.

1.3. Purpose of this document

The purpose for this document is to provide supervisory guidance regarding the assessment of TLPT providers under Article 7 of the RTS on TLPT, see **Annex I**.

In particular, this document seeks to support FEs, TLPT providers, and relevant competent authorities in assessing whether prior experience obtained under recognised non-EU threat intelligence-led testing frameworks may be considered when demonstrating relevant expertise, capabilities, and previous assignments for the purposes of Article 7 of the RTS on TLPT, see **Annex I**.

This document does not establish additional regulatory requirements nor replace obligations arising under the DORA Regulation, the RTS on TLPT, or the TIBER-EU framework as well as its guidance documents. Rather, it aims to facilitate a consistent and risk-based approach to the assessment of equivalent or comparable experience across recognised frameworks.

1.4. Target Audience

This document is intended for:

- TLPT providers participating in or seeking to participate in TLPT engagements;
- testers and threat intelligence providers with experience under recognised testing frameworks outside the TIBER-EU framework;
- FEs responsible for selecting and assessing TLPT providers pursuant to Article 9(11) of the RTS on TLPT;
- competent authorities considered as the TLPT and/or TIBER authority.

2. Methodology and Limitations

2.1. Methodology

This document adopts a comparative horizontal assessment approach using the TIBER-EU framework as the reference baseline against selected non-EU threat intelligence-led testing frameworks, see *table 1*. Other non-EU frameworks, such as ASSURE, GBEST, and NCSC (CHECK), were excluded from the assessment.

Non-EU framework within the scope of this document	Description
CBEST	A United Kingdom based cyber security testing ('CBEST')[6] threat intelligence-led assessment developed by the Bank of England.
iCAST	Intelligence-led cyber attack simulation testing ('iCAST')[7] developed by the Hong Kong Monetary Authority.
AASE	Adversarial Attack Simulation Exercise ('AASE')[8] developed by the Association of Banks in Singapore.
I-CRT	Intelligence-led cyber resilience testing ('I-CRT')[9] assessment developed by the Superintendent of Financial Institutions based in the Canadian jurisdiction.

Table 1: List of relevant non-EU frameworks covered in the Mapping Exercise

The assessment focuses on identifying similarities and differences in governance arrangements, process structure, stakeholder roles, testing phases, and associated deliverables across the selected frameworks, through a mapping exercise, see **Annex II** – *table 3*. To support consistency of assessment, predefined classification criteria were applied to determine the degree of alignment between framework requirements, see **Annex II** – *table 4*.

The mapping exercise was conducted through a structured assessment of corresponding framework requirements, chapters, sections, and processes, see **Annex III**. Additionally, the assessment shall compare the various key words of the stakeholders between framework, see **Annex IV**.

The objective of the assessment is not to establish regulatory equivalence between frameworks but rather to assess whether practical experience obtained under such frameworks may demonstrate comparable competencies relevant to TLPT engagements.

[6] CBEST Threat Intelligence-Led Assessments | Bank of England
[7] 5fecc1fe13498132b4fa835b_HKMA CFI - Cyber Resilience Assessment Framework - Dec 2016.pdf
[8] AASE Final new 2
[9] OSFI's Intelligence-led Cyber Resilience Testing (I-CRT) Framework - Office of the Superintendent of Financial Institutions

2.2. Limitations

This document should be read together with the DORA Regulation and its RTS on TLPT, as well as the TIBER-EU framework, CBEST, iCAST, AASE, and I-CRT.

The assessment within this document is limited to the extent to which the respective frameworks contain processes, governance arrangements, stakeholder roles, and deliverables corresponding to the preparation, testing, and closure phases of the TIBER-EU framework.

The mapping exercise does not constitute a determination of regulatory equivalence between frameworks and inclusion within this analysis should not be interpreted as constituting automatic fulfilment of Article 7 of the RTS on TLPT requirements, see **Annex I**.

Consequently, FEs and competent authorities should continue to undertake case-by-case assessments of TLPT providers and exercise appropriate professional judgement, in accordance with Article 9(11) of the RTS on TLPT.

3. Key Observations

The mapping exercise, see **Annex II** – *table 3*, indicates that, among the non-EU frameworks assessed, CBEST and I-CRT demonstrate the strongest degree of alignment with the TIBER-EU framework. Both frameworks contain a more developed supervisory component and include processes that correspond to key TIBER-EU phases. In particular:

- CBEST is assessed as strongly aligned or complementary across several mapped areas. This is primarily due to its regulator-led nature and the presence of structured requirements similar to the TIBER-EU framework's preparation phase, testing phase, and closure phase. The mapping exercise also indicates limited partial alignment between CBEST and the TIBER-EU framework. In addition, CBEST service providers are required to be CREST-approved accredited service providers, which may be relevant when considering professional capability, market recognition, and prior experience for the purposes of Article 7 of the RTS on TLPT, see **Annex I**.
- I-CRT is assessed as strongly aligned or complementary across several mapped areas, particularly due to the role of the Office of the Superintendent of Financial Institutions in initiating, overseeing, and following up on the assessment, see **Annex IV**. The mapping exercise further indicates only limited partial alignment between I-CRT and the TIBER-EU framework. I-CRT therefore provides a closer comparison to the TIBER-EU framework than frameworks where the relevant authority does not perform a direct supervisory role throughout the assessment lifecycle.

By contrast, iCAST and AASE, while containing relevant threat intelligence-led and adversarial testing components, differ from the TIBER-EU framework in their governance and supervisory arrangements resulting in multiple partial alignment. In particular:

- iCAST is embedded within the Hong Kong Monetary Authority's Cyber Resilience Assessment Framework ('C-RAF'). While iCAST contains relevant threat intelligence and cyber attack simulation elements, the exercise is not structured as a regulator-led framework in the same manner as the TIBER-EU framework. This distinction affected the mapping exercise and resulted in multiple partial alignment as well as multiple processes and deliverables within the TIBER-EU framework not expressly addressed.
- AASE, while containing relevant threat intelligence and cyber attack simulation elements, is not structured as a regulator-led framework in the same manner as the TIBER-EU framework. This distinction affected the mapping exercise and resulted in multiple partial alignment as well as some certain deliverables within the TIBER-EU framework not expressly addressed.

Therein above, threat intelligence providers and testers with experience under the selected non-EU frameworks may provide such experience as supporting evidence for

assessment by FEs and competent authorities under Article 7 of the RTS on TLPT, see **Annex I**, where comparable competencies and practical experience can be demonstrated.

4. Annex

4.1. Annex I: RTS on TLPT, Article 7, Selection of TLPT Providers

Ref		
1.		The control team shall take measures to manage the risks relating to the TLPT and shall in particular ensure that, for each TLPT
	(a)	the threat intelligence provider and external testers provide the control team with a detailed *curriculum vitae* and copies of certifications that, according to recognised market standards, are appropriate for the performance of their activities;
	(b)	the threat intelligence provider and external tester are duly and fully covered by proper professional indemnity insurances including against risks of misconduct and negligence;
	(c)	the threat intelligence provider provides at least three references from previous assignments in the context of penetration testing and red team testing;
	(d)	the external testers provide at least five references from previous assignments related to penetration testing and red team testing;
	(e)	the staff of the threat intelligence provider assigned to the TLPT:
		(i) is composed of at least a manager with at least 5 years' experience in threat intelligence and at least one additional member with at least 2 years' experience in threat intelligence;
		(ii) display a broad range and appropriate level of professional knowledge and skills, including: (1) intelligence gathering tactics, techniques and procedures; (2) geopolitical, technical and sectorial knowledge; (3) adequate communication skills to clearly present and report on the result of the engagement;
		(iii) has a combined participation in at least three previous assignments in threat intelligence in the context of penetration testing and red team testing;
		(iv) does not simultaneously perform any blue team tasks or other services that may present a conflict of interest with respect to the financial entity, ICT third-party service provider or an ICT intra-group service provider involved in TLPT to which they are assigned;
		(v) is separated from and not reporting to staff of the same TLPT provider providing external testers for the same TLPT;
	(f)	for external testers, the red team assigned to the TLPT:
		(i) is composed of at least a manager, with at least 5 years of experience in penetration testing and red team testing as well as at least two additional testers, each with penetration testing and red team testing of at least 2 years;
		(ii) displays a broad range and appropriate level of professional knowledge and skills, including knowledge about the business of the financial entity, reconnaissance, risk management, exploit development, physical penetration, social engineering, vulnerability analysis, as well as adequate communication skills to clearly present and report on the result of the engagement;
		(iii) has a combined participation in at least five previous assignments related to penetration testing and red team testing;
		(iv) is not employed by, nor provides services to, a threat intelligence provider that simultaneously performs blue team tasks for either a financial entity, an ICT

		third-party service provider, or an ICT intra-group service provider that is involved in the TLPT;
		(v) is separated from any staff of the same TLPT provider that simultaneously provides threat-intelligence services for the same TLPT;

Table 2: Article 7(1)(a) to (f) of the RTS on TLPT

4.2. Annex II: Mapping Exercise of Interplay between the TIBER-EU Framework and relevant Non-EU Frameworks

	TIBER-EU Framework Requirements	CBEST	iCAST	AASE	I-CRT
	Identification of entity to be in scope of a TIBER test				
Preparation Phase	Notification to start a TIBER test				
	Initiation Information				
	Contacting Providers				
	Scope Specification Document				
	Initial Risk Assessment & Management				
Testing Phase	Threat Intelligence collection and Threat Scenario				
	Targeted Threat Intelligence Report				
	Red Team Test Plan				
	Updated Risk Assessment & Management				
	Active Testing				
Closure Phase	Red Team Test Report				
	Blue Team Test Report				
	Replay Exercise				
	Purple Teaming Exercise				
	360 Feedback Meeting				
	Test Summary Report				
	Remediation Plan				
	Attestation				
	Remediation Process				

Table 3: Annex II.A Matrix mapping exercise of interplay between the TIBER-EU framework and relevant non-EU frameworks

	Fully aligned	The framework contains substantially equivalent objectives, processes, and outcomes.
	Complementary	The framework contains provisions which support or supplement the relevant TIBER-EU requirement.
	Partially aligned	The framework contains similar concepts or objectives but differs in implementation or scope.
	Not addressed	The framework does not explicitly address the relevant requirement.

Table 4: Annex II.B Matrix mapping exercise of interplay between the TIBER-EU framework and relevant non-EU frameworks

4.3. Annex III: Summary of Non-EU Frameworks Chapter, Section, and Paragraph Requirements relevant to the TIBER-EU Framework

TIBER-EU Framework Process	TIBER-EU Framework Reference	Other framework requirements
Identification	Chapter 2.2.3	**CBEST**: Section 3 (CBEST overview) 3.1 **iCAST**: Chapter 1. (Overview) 1.1.4.; Chapter 4. (intelligence-led Cyber Attack Simulation Testing (iCAST)) 4.1.5. **AASE**: Section 4 (Definitions) Letter of Engagement; Section 7 (Methodology) 7.1.6.4 **I-CRT**: Section 2. (Introduction) 2.2.6
Notification	Chapter 6.2	**CBEST**: Section 6 (Initiation phase) 6.1, 6.2 **iCAST**: Chapter 1. (Overview) 1.1.4.; Chapter 4. (intelligence-led Cyber Attack Simulation Testing (iCAST)) 4.1.5. **AASE**: Section 4 (Definitions) Letter of Engagement; Section 7 (Methodology) 7.1.6.4 **I-CRT**: Section 5. (I-CRT process) 5.1.1, 5.1.2
Initiation	Chapter 6.3	**CBEST**: Section 6 (Initiation phase); Section 3 (CBEST overview) 3.2.2 **iCAST**: N/A **AASE**: Section 7 (Methodology) 7.1.1, 7.1.2, 7.1.6; Section 8 (Appendix) 8.1.1 **I-CRT**: Section 5. (I-CRT process) 5.1.2
Scoping	Chapter 6.4	**CBEST**: Section 6 (Initiation phase) 6.1, 6.3 **iCAST**: Chapter 4. (intelligence-led Cyber Attack Simulation Testing (iCAST)) 4.5. **AASE**: Section 7 (Methodology) 7.1.1, 7.1.2; Section 8 (Appendix) 8.1.1 **I-CRT**: Section 5. (I-CRT process) 5.1.3
Procurement	Chapter 6.5	**CBEST**: Section 6 (Initiation phase) 6.2, 6.4, 6.4.1, 6.4.2, 6.4.3 **iCAST**: Chapter 5. (Qualification requirements) 5.3.1. **AASE**: Section 7 (Methodology) 7.1.4 **I-CRT**: Section 5. (I-CRT process) 5.1.4
Risk Assessment and Mitigation	Chapter 4	**CBEST**: Section 5 (CBEST risk management); Section 6 (Initiation phase) 6.3 **iCAST**: N/A **AASE**: Section 7 (Methodology) 7.1.2, 7.1.3; Section 8 (Appendix) 8.1.1

		I-CRT: Section 4. (Risk management); Section 5. (I-CRT process) 5.1.2, 5.3.1.
Key considerations for the Threat Intelligence Provider	Chapter 7.2	**CBEST**: Section 3 (CBEST overview) 3.2.5; Section 7 (Threat Intelligence phase) 7.2.1, 7.2.2 **iCAST**: Chapter 4. (intelligence-led Cyber Attack Simulation Testing (iCAST)) 4.6.1., 4.6.2., 4.6.3., 4.6.4. **AASE**: Section 7 (Methodology) 7.2.1, 7.2.2. **I-CRT**: Section 2. (Introduction) 2.2.3; Section 5. (I-CRT process) 5.2.1, 5.2.2
Scenario creation	Chapter 7.3	**CBEST**: Section 7 (Threat Intelligence phase) 7.2.3 **iCAST**: Chapter 4. (intelligence-led Cyber Attack Simulation Testing (iCAST)) 4.6. **AASE**: Section 7 (Methodology) 7.2.3; Section 8 (Appendix) 8.1.2 **I-CRT**: Section 5. (I-CRT process) 5.2.2
Targeted Threat Intelligence Report creation	Chapter 7.4	**CBEST**: Section 7 (Threat Intelligence phase) 7.2.4, 7.3, 7.4 **iCAST**: Chapter 4. (intelligence-led Cyber Attack Simulation Testing (iCAST)) 4.6.5., 4.6.6., 4.6.7., 4.6.8., 4.6.9., 4.9.4., 4.9.3. **AASE**: Section 7 (Methodology) 7.2.2.1, 7.2.2.2, 7.2.2.3; Section 8 (Appendix) 8.1.2, 8.1.2.1, 8.1.2.2 **I-CRT**: Section 5. (I-CRT process) 5.2.2, 5.2.3, 5.2.4
Key considerations for the Red Team Testers	Chapter 8.2	**CBEST**: Section 8 (Penetration Testing phase) 8.2 **iCAST**: Chapter 4. (intelligence-led Cyber Attack Simulation Testing (iCAST)) 4.6.5. **AASE**: Section 7 (Methodology) 7.3.1 **I-CRT**: Section 2. (Introduction) 2.2.2, 2.2.4; Section 5. (I-CRT process) 5.3.1, 5.3.2
Red Team Test Plan creation	Chapter 8.3	**CBEST**: Section 8 (Penetration Testing phase) 8.1 **iCAST**: Chapter 4. (intelligence-led Cyber Attack Simulation Testing (iCAST)) 4.7.1., 4.7.2. **AASE**: Section 7 (Methodology) 7.3.1; Section 8 (Appendix) 8.1.3 **I-CRT**: Section 5. (I-CRT process) 5.3.1
Active testing	Chapter 8.4	**CBEST**: Section 8 (Penetration Testing phase) 8.2 **iCAST**: Chapter 4. (intelligence-led Cyber Attack Simulation Testing (iCAST)) 4.8.1., 4.8.2. **AASE**: Section 7 (Methodology) 7.3.2, 7.3.3, 7.3.4, 7.3.5, 7.3.6, 7.3.7, 7.3.8, 7.3.9 **I-CRT**: Section 5. (I-CRT process) 5.3.2
Red Team Test Report and Blue	Chapter 9.2	**CBEST**: Section 8 (Penetration Testing phase) 8.4 **iCAST**: Chapter 4. (intelligence-led Cyber Attack Simulation Testing (iCAST)) 4.9.1., 4.9.2., 4.9.4.

Team Test Report creation		**AASE**: Section 7 (Methodology) 7.4.1, 7.4.2, 7.4.4; Section 8 (Appendix) 8.1.4, 8.1.5, 8.1.6, 8.1.7 **I-CRT**: Section 5. (I-CRT process) 5.3.3, 5.3.4
Replay exercise	Chapter 9.3	**CBEST**: Section 8 (Penetration Testing phase) 8.3; Section 7 (Threat Intelligence phase) 7.4 **iCAST**: N/A **AASE**: Section 7 (Methodology) 7.4.3 **I-CRT**: Section 5. (I-CRT process) 5.3.3
Purple Teaming exercise	Chapter 9.4	**CBEST**: Section 8 (Penetration Testing phase) 8.3; Section 7 (Threat Intelligence phase) 7.4 **iCAST**: N/A **AASE**: Section 7 (Methodology) 7.4.3 **I-CRT**: N/A
Test Summary Report	Chapter 9.5	**CBEST**: N/A **iCAST**: N/A **AASE**: N/A **I-CRT**: N/A
Remediation plan	Chapter 9.6	**CBEST**: Section 9 (Closure phase) 9.1, 9.3 **iCAST**: Chapter 4. (intelligence-led Cyber Attack Simulation Testing (iCAST)) 4.9.4. **AASE**: Section 7 (Methodology) 7.4.5; Section 8 (Appendix) 8.1.8 **I-CRT**: Section 5. (I-CRT process) 5.4.1
360 feedback	Chapter 9.7	**CBEST**: Section 9 (Closure phase) 9.2 **iCAST**: N/A **AASE**: Section 7 (Methodology) 7.4.6 **I-CRT**: N/A
Attestation, result dissemination and follow-up	Chapter 9.8	**CBEST**: Section 9 (Closure phase) 9.1 **iCAST**: Chapter 4. (intelligence-led Cyber Attack Simulation Testing (iCAST)) 4.9.1., 4.9.2., 4.9.4. **AASE**: Section 7 (Methodology) 7.4.5; Section 8 (Appendix) 8.1.8 **I-CRT**: Section 5. (I-CRT process) 5.4.1, 5.4.2

Table 5: Annex III Summary of non-EU frameworks chapter, section, and paragraph requirements relevant to the TIBER-EU framework

4.4. Annex IV: Summary of Non-EU Frameworks Stakeholders relevant to the TIBER-EU Framework

Key word comparison				
TIBER-EU framework	**CBEST**	**iCAST**	**AASE**	**I-CRT**
Control Team Lead	Control Group Co-ordinator	Control Group	Exercise Director	Control Group Coordinator
Control Team	Control Group			Federally Regulated Financial Institution and Federally Regulated Financial Institution Control Group
TIBER Authority	Regulator	N/A		Office of the Superintendent of Financial Institutions
TIBER Control Team				Regulator
Test Manager				
Internal Red Team Testers	N/A	N/A	Attacker or Red Team	N/A
External Red Team Testers	Penetration Test Service Provider	iCAST Team		Red Team service Provider
Threat Intelligence Providers	Threat Intelligence Service Providers	Threat Intelligence Team		Threat Intelligence service Provider
Blue Team	N/A	Incident Response Team	Defender or Blue Team	Defenders or Blue Team

Table 6: Annex IV Summary of non-EU frameworks stakeholders relevant to the TIBER-EU framework

Malta Financial Services Authority

Triq L-Imdina, Zone 1

Central Business District, Birkirkara, CBD 1010, Malta

communications@mfsa.mt

www.mfsa.mt