European Association of CCP Clearing Houses

# EACH Response – ESAs consultation on Draft RTS specifying elements related to threat led penetration tests

March 2024


European Association of CCP Clearing Houses AISBL (EACH), Avenue des Arts 6, 1210 Brussels

## Introduction

The European Association of CCP Clearing Houses (EACH) represents the interests of Central Counterparties (CCPs) in Europe since 1992. CCPs are financial market infrastructures that significantly contribute to safer, more efficient and transparent global financial markets. EACH currently has 18 Members from 14 different European countries. EACH is registered in the European Union Transparency Register with number 36897011311-96.

EACH appreciates the opportunity to provide feedback to the consultation paper on Draft RTS elements related to threat led penetration tests (TLPT)[1].

As an introductory comment, EACH would like to underline that the **timeline for the implementation of DORA** (which will apply from 17 January 2025) **appears to be extremely challenging**. EACH Members are calling for an **extension of such timeline** in order to ensure a smooth and **efficient implementation**. We would expect Authorities to provide comfort to the industry accordingly as well as some **prioritisation** of the aspects of DORA that should be implemented first.

## Questions

**Q1. Do you agree with this cross-sectoral approach? If not, please provide detailed justifications and alternative wording as needed.**

Yes, EACH Members **agree with the cross-sectoral approach** proposed in the consultation document.

**Q2. Do you agree with this approach? If not, please provide detailed justifications and alternative wording as needed.**

Yes, EACH Members **agree with the proportionality approach** proposed in the consultation document. However, we would like to kindly request a **clarification regarding the concept of "ICT maturity" in paragraph 22**. We would appreciate more clarity on when a financial entity could be considered "mature enough from an ICT perspective" to perform a TLPT.

**Q3. Do you agree with the two-layered approach proposed to identify financial entities required to perform TLPT? If not, please provide detailed justifications and alternative wording as needed**.

Yes, EACH Members **agree with the two-layered approach** proposed to identify financial entities required to perform TLPT.

[1] https://www.esma.europa.eu/sites/default/files/2023-12/JC_2023_72_-_CP_on_draft_RTS_on_TLPT.pdf

**Q4. Do you agree with the proposed quantitative criteria and thresholds in Article 2(1) of the draft RTS to identify financial entities required to perform TLPT? If not, please provide detailed justifications and alternative wording as needed.**

We consider that **Article 2(1)(f) is not sufficiently clear in relation to which trading venues are in scope**. The measurement of market share at the national level should be with reference to market participants in that Member State and the venue with the highest share for one Member State could be located anywhere in the Union. The alternative interpretation of identifying the largest turnover venue in each Member State will lead to disproportionate efforts for limited outcomes in terms of including potentially very small domestic venues in scope.

**Q5: Do you consider that the RTS should include additional aspects of the TIBER process? If so, please provide suggestions**.

EACH Members consider that **additional aspects of the TIBER process are not necessary**.

**Q6. Do you agree with the approach followed for financial entities to assess the risks stemming from the conduct of testing by means of TLPT? If not, please provide detailed justifications and alternative wording as needed**.

EACH Members **agree with the proposed approach**.

**Q7. Do you consider the proposed additional requirements for external testers and threat intelligence providers are appropriate? If not, please provide detailed justifications and alternative wording or thresholds as needed**.

EACH Members suggest that **external testers and threat intelligence providers should prove their experience not only in TLPT, but also in TLPT *in the financial sector***.

Requesting three and five references from previous assignments related to intelligence-led red team tests poses challenges. The nature of such engagements often demands a high-level of confidentiality to preserve the effectiveness of the assessments. Disclosing specific details about prior assignments could compromise the anonymity and security of the clients involved.

Also, organizations seeking such services may face challenges finding vendors with a well-established track record in the relatively new domain of threat-led penetration testing in the EU cybersecurity landscape.

**Q8. Do you think that the specified number of years of experience for external testers and threat intelligence providers is an appropriate measure to ensure external testers and threat intelligence providers of highest suitability and reputability and the appropriate knowledge and skills? If not, please provide detailed justifications and alternative wording as needed**.

EACH would like to understand **how this would be monitored**. As an example, whether the TLPT would be considered invalid if, only after it is performed, it is verified that the manager of the threat intelligence provider assigned to the TLPT only has 4 years of experience instead of the required 5 years. We would also kindly request **clarification on what kind of paperwork shall the financial entity provide the regulator within this context**.

Furthermore, the **specified numbers of years of experience for external testers and threat intelligence providers will present difficulties** in finding the right external vendors, with such experiences. It would highly increase the cost of the overall TLPT.

**Q9. Do you consider the proposed process is appropriate? If not, please provide detailed justifications and alternative wording as needed**.

EACH Members would like to put forward the following comments:

- **Article 6(1)** – The financial entity is required to 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. However, it appears that **there is no deadline for the assessment and validation from the TLPT authority's side**. EACH would like to kindly ask a **clarification regarding what would happen if e.g. the TLPT authority does not approve the selected external testers or threat intelligence provider**. In case of non-approval, the preparation period would require more than the proposed three months. Furthermore, the TIBER-EU framework provides a longer notice time of almost 12 months. **Three-month notice seems to be a short period of time**.
- **Article 6(4)** – Given that the scope specification document can only be prepared and submitted to the TLPT authority after the initiation documents have been validated/approved, the **deadline for submitting the scope specification document should therefore consider this dependency** and the submission to the TLPT authority should be defined as **three months after the TLPT authority has approved** the scope specification document.
- **Article 6(9)** – This Article requires the TLPT authority to inform the financial entity of their approval of the scope specification document. However, **no timing is foreseen for the TLPT authority to perform such exercise**. We would like to kindly ask that such timing for the TLPT authority is added.
- **Article 7(3)** – Based on the TIBER framework, the threat intelligence team comes up with the scenarios together with central banks. DORA states that control team chooses the scenario themselves. It would be beneficial to **have the same requirement**.
- **Article 7(6) and Article 8(1)** – Similarly as per Art. 6(9), we suggest including a **deadline for the TLPT authority** to inform the financial entity of their approval.
- **Article 8(5)** – The duration of a TLPT may vary depending on the size of the CCP, the services they offer, the products they clear, etc. Therefore, if the scope and complexity of the financial entity is considered, there should be **no minimum duration for a TLPT defined**, and **12 weeks for a small entity seems to be too demanding** in terms of resources and costs. The duration of the active red team testing phase shall be at least **minimum 12 weeks and maximum 16 weeks**.

- **Article 9(7)** – Within 12 weeks from completion of active red team testing, the control team shall submit the test summary report to the TLPT authority for approval. TIBER provides 16 weeks, where DORA provides only 12. We kindly suggest for the requirement to **remain the same based on the TIBER-EU framework**.
- **Article 10(2c, 2d)** – This Article states that remediation plan must provide information on root cause analysis and the financial entity's staff or functions responsible for the implementation of the proposed remediation measures or improvements. Such requirement means asking companies to provide highly sensitive information. We would therefore kindly request **ESAs to consider making changes for this specific request**.

**Q13. Do you have any other comment or suggestion to make in relation to the proposed draft RTS? If so, please provide detailed justifications and alternative wording as needed**.

Smaller CCPs tend to have their IT systems provided ICT TPPs. Often the office IT infrastructure is subject to a Software-as-as-service (SaaS) contract and even managed notebooks and other devices are provided and managed by a ICT TPP.

To avoid high costs and unnecessary burden to the financial entity for preparing and managing the tests and to recognize the above specific situation and requirements, **financial entities should be allowed to rely on TLPTs that are performed by ICT TPPs**. Prerequisite should be that all critical or important functions are covered by such TLPTs, that only external TLPT testers are allowed and that the test reports and related remediation plans are shared with the financial entity.

We would also ask the regulators to provide **specific guidance on the classification of TLPT reports and how they would be authorized**. It is important to avoid misclassification of these reports.