Brussels, 1 March 2024

FINAL - CDO

EACB comments on

Draft Regulatory Technical Standards specifying elements related to threat led penetration tests

General drafting principles

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

Q2: Do you agree with the proposed approach on proportionality? If not, please provide detailed justifications and alternative wording as needed

Approach on the identification of financial entities required to perform 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.

Generally speaking, some of our members have been informed by their national competent authorities that the authorities will individually notify the FEs obligated to perform TLPTs, excluding those who are exempted or not selected. This implies that the latter group may remain unaware of their exemption status. We suggest that the RTS explicitly state that the authority should be responsible for informing all FEs, both those obligated to perform the TLPT and those exempted from the requirement.

Our second remark pertains to Art. 2.3 (a) and (b) of the RTS. We find that the ICT-risk-related factors (b) are relatively broadly formulated. If utilised as standalone criteria, many FEs could be subject to TLPTs. For instance, the dependence of critical and important functions on ICT is always high. Therefore, we recommend using a combination of factors from both (a) 'impact-related and systemic character related factors' and (b) 'ICT risk-related factors' to determine the affected FI. For example, these criteria could be categorised as low/medium/high, and only if both criteria in (a) and (b) are rated as high should the financial institution be considered eligible for a TLPT.

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.

EACB AISBL – Secretariat • Rue de l'Industrie 26-38 • B-1040 Brussels
Tel: (+32 2) 230 11 24 • Fax (+32 2) 230 06 49 • Enterprise 0896.081.149 • lobbying register 4172526951-19
www.eacb.coop • e-mail : secretariat@eacb.coop

Approach on the testing: scope, methodology, conclusion

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

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.

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.

In general, there are very few providers currently meeting all the listed criteria, resulting in a highly restricted market. This poses a dual risk: European financial institutions might become overly reliant on a limited number of providers, granting them extensive insights into institutional vulnerabilities. Conversely, even Threat-Led Penetration Tests (TLPTs) face potential jeopardy, as financial institutions may struggle to find suitable providers. The stringent requirements may exclude numerous well-established threat intelligence and red team providers in each Member State from conducting TLPTs. Many threat intelligence companies, for example, those that conducted TIBER-EU Tests, might encounter challenges in proving the necessary threat intelligence experience in the financial sector. Similarly, numerous red team providers that performed TIBER-EU Tests may face difficulties demonstrating the required experience in 'threat intelligence-led' red team tests. We propose that the TLPT Authority consider the possibility of permitting providers who do not fulfill every aspect of the specified requirements to participate.

We recommend incorporating a degree of flexibility and adaptability to the evaluation process, granting the financial entity the possibility to determine the most appropriate vendors for TLPTS testers and Threat Intelligence services. This approach will allow for a more nuanced and tailored selection of vendors, enhancing the likelihood of identifying those best suited for the FE's specific testing requirements and threat intelligence needs. Strict adherence to all criteria might limit the pool of available providers, and allowing some flexibility could be beneficial for the testing process.

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.

Competency assessments based on experience over time require careful examination. While the number of years of experience serves as an indicator of competence, it should not be obligatory if proficiency can be adequately substantiated through project evidence, publications (presentations), and certifications. Additionally, acquiring verifiable evidence from service providers poses a challenge. Service providers typically operate on a project-by-project basis, making it impractical for them to showcase experience on an annual basis, especially considering that many projects have a duration of less than a year.

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

Q10: Do you consider the proposed requirements for pooled testing are appropriate? If not, please provide detailed justifications and alternative wording as needed.

The proposed procedure for pooled testing lacks clarity. Unfortunately, the current DORA requirement stating that pooled audits may only be conducted by ICT service providers whose customers from other sectors could potentially be affected disproportionately benefits large cloud providers. This could incentivise providers to include customers not impacted by DORA solely to avoid the risks and substantial effort associated with non-pooled testing.

To address this, the RTS should provide more detailed specifications on how pooled audits are to be organised. If the supervisory authority does not publicly disclose the financial institutions obligated to perform TLPT or only communicates this information to individual institutions, the TLPT plans of these institutions become entirely reliant on ICT service providers. These providers hold exclusive knowledge of which financial institutions have requested inclusion in TLPT. It is crucial for financial institutions to take the lead in this process, allowing them to coordinate their requirements and plans for pooled audits in collaboration with service providers.

Approach on the use of internal testers

Q11: Do you agree with the proposed requirements on the use of internal testers? If not, please provide detailed justifications and alternative wording as needed.

Approach on cooperation

Q12: Do you consider the proposed requirements on supervisory cooperation are appropriate? If not, please provide detailed comments and alternative wording as needed.

Final comments

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

Contact:

For further information or questions on this paper, please contact:

- Ms Marieke van Berkel, Head of Department Retail Banking, Payments, Digitalisation and Financial Markets (marieke.vanberkel@eacb.coop)
- Ms Chiara Dell'Oro, Senior Adviser for Digital Policies (chiara.delloro@eacb.coop)