ESMA
Securities and Markets Stakeholder Group

EIOPA - IRSG

eba European Banking Authority
BANKING STAKEHOLDER GROUP

JC 2024 17

12 03 2024

Joint European Supervisory Authority Consultation paper on Draft Regulatory Technical Standards specifying elements related to threat led penetration tests

Background

The Digital Operational Resilience Act (DORA) mandated the European Supervisory Authorities (EBA, EIOPA and ESMA – the ESAs) to jointly develop policy instruments, including technical standards, to ensure a consistent and harmonized legal framework in the areas of ICT risk management, major ICT-related incident reporting and ICT third-party risk management for all EU financial entities.

The second batch, that is open for consultation until 4 March 2024, comprises the following:

- RTS and ITS on content, timelines and templates on incident reporting
- GL on aggregated costs and losses from major incidents
- RTS on subcontracting of critical or important functions
- RTS on oversight harmonisation
- GL on oversight cooperation between ESAs and competent authorities
- RTS on threat-led penetration testing (TLPT).

General comments

The Stakeholder Groups (SGs) welcome the opportunity to comment on the *"Draft Regulatory Technical Standards specifying elements related to threat led penetration tests".*

In our response, the SGs focus only on those elements that we feel competent enough to provide meaningful input.

Questions for consultation

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

The SGs agree, in principle, with the proposed approach, subject to the following observations:

The SGs note, that TIBER-EU has yet to publish comprehensive guidance for combined TLPTs with individual financial entities (FEs) and ICT third party providers (TPPs) (Article 26(3) DORA), or for pooled tests with multiple FEs or TPPs (Article 26(4) DORA). The RTS makes reference to these tests, as per the DORA Level 1 text, but does not provide further guidance concerning their operationalisation. Both forms of test involve a significant degree of complexity, with material legal, operational and practical challenges that have yet to become established norms within the financial or technology sectors. The financial entity, who would be accountable for administering both tests, would face significant risk if they were required by a TLPT authority to do a combined or pooled test. There is a risk that not all stages of the TLPT required by the RTS would be completed and the expected timelines set out in the RTS may not adequately account for the complexity of either test. Further guidance concerning combined or pooled TLPT tests should be obtained before such tests could be completed in practice.

Some members of the SGs note that the RTS introduces mandatory 'purple teaming', which is an optional element of TIBER-EU and not a stated requirement in DORA Level 1. They suggest that a mandatory 'purple team' exercise after an external test which indicated limited to no vulnerabilities would not add value to the external testing team or the FE. They recommend, therefore, that 'purple teaming' should only be required when a sufficient number of vulnerabilities are demonstrated in the 'red/blue teaming' exercise. Other members believe that there could be other situations where 'purple teaming' is not required and would recommend that it should be encouraged but made optional altogether.

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

The SGs agree with the ESAs approach in general. Some members of the SGs believe that the RTS should allow for more flexibility in certain areas given the diverse set of financial entities covered by DORA and the fact that their existing capabilities and experience with TLPT may also differ widely. Article 2(1) RTS sets out the criteria for identifying FEs that would be in scope to complete TLPT under DORA. The SGs agree with the criteria, which are based on definitions and metrics used elsewhere in relevant sectoral legislation to identify 'significant' or 'systemically important' entities. Some members of the SGs have expressed concerns that the number of institutions obliged to conduct testing may be such that it could cause practical challenges, e.g. with testing capacities, especially given the required frequency of testing. The SGs welcome the suggestion that competent authorities should retain a degree of discretion to assess the appropriateness of TLPT on a case-by-case basis ((Article 2(2) RTS) and to selectively 'opt out' FEs from the requirement.

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.

The SGs agree with the two-layered approach and welcome the approach that membership of a corporate groups should be taken into account in the identification of FEs subject to TLPT. Where ICT systems are shared across different legal entities of the same group, group testing would be preferred. For FEs which belong to a group where the parent undertaking is located outside the

EU, and which operate in the EU with more than one subsidiary or significant branch, the designation of a TLPT authority in one member state as the lead-EU TLPT authority may be warranted.

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.

The SGs agree, in principle, with the proposed approach, subject to the following observations:

- Some members of the SGs are of the view that the threshold for payment institutions set at EUR 120 billion of total value payment transactions appears low and should perhaps be changed in a way that provides more flexibility for authorities to decide when to include FE in the testing.

- Some members of the SGs are of the view that the criteria for determining insurance and reinsurance undertakings to be in scope of TLPT in Article 2(1)(g) are not sufficient for companies to know whether they are in scope or not. They note that this information is not publicly available, or not available at all (calculations per activity area), so that companies may not be able to calculate objectively whether they would be in scope. They suggest that further clarification may be needed on the criteria, especially specifying the relationships between the clauses (e.g. 10% of total assets, or overall assets in one area).

- Some members of the SGs consider that the envisaged timelines for TLPTs may not be in line with practical experience so far, especially if the inclusion of mandatory 'purple teaming' is kept and suggest that a less prescriptive approach may be warranted.

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

The SGs generally welcome the intended alignment with the TIBER-EU framework and appreciate the limitations inherent in incorporating the original, voluntary framework into a regulatory text. Some members of the SGs note that additional aspects of the TIBER-EU framework may be included in the form of guidance rather than mandatory obligations. These members argue that this approach would better reflect proportionality considerations and a risk-based approach towards testing and avoid undue burden on financial entities.

Annex II 2(a) requires FEs to provide a list of all critical or important function and to explain on which basis a critical or important function is or is not to be included in the scope of the proposed TLPT exercise. In practice, FE usually choose a small subset of critical or important functions for inclusion in the TLPT exercises. Annex II 2(a) would therefore likely require a long list of explanations. In the interest of efficiency, the structure of Annex II could be streamlined to focus on the initial list of critical or important functions, the subset of functions included in the TLPT, and the methodology applied in selecting that sample.

It may be beneficial to develop a set of guidelines for additional aspects that go beyond the existing TIBER framework, for example on combined and pooled testing, to provide guidance to FEs on how to apply these new requirements.

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.

The SGs broadly agree with the proposed approach. Some members of the SGs are of the view, however, that the mandatory nature of the requirements in Article 5 may present an undue burden on financial institutions and may be counterproductive and detrimental to the successful completion of TLPT. These members recommend including optionality for financial entities when listing requirements in items (a) to (g) of Article 5(2) and suggest that the wording in Article 5(2) should be amended to read: "The control team shall consider taking measures to manage risks…", instead of "The control team shall take measures…".Similarly, these members suggest that item (h) of Article 5(2) should give optionality to the FE's control team to consider additional restoration procedures with the testers, instead of mandating all the measures listed in the draft RTS. Other members of the SGs observe, however, that divergences in the practical implementation of TLPT testing, especially with regard to risk management measures, could run counter to the legislators' original intent of promoting a consistent methodology and ensuring uniformly high standards of security.

Some members of the SGs believe that FAs should be able to share the risk assessment findings inside their own organisation without being constrained excessively by confidentiality provisions. Other members of the SGs suggest that, instead, the control team should assign relevant roles to help process and distribute findings from the risk-assessment.

Some members of the SGs note that the FE should also be allowed to pause the TLPT in case of a real world attack during the test. Other members note that this scenario should be adequately covered by Article 8(10) RTS.

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.

The SGs consider the requirements broadly appropriate. Some members of the SGs are of the view that the mandatory nature of the requirements in Article 5 may present an undue burden on financial institutions and may be counterproductive and detrimental to the successful completion of TLPT (see Q6. above). These members of the SGs suggest amendments, in particular to items (a), (c), (d) and (f) of Article 5, to reflect some optionality for financial entities to have the ability to make exceptions after having performed an internal risk-assessment and listed relevant mitigating factors. They note, for example, that the obligation to request three references for threat intelligence provider (item c) and five references for external testers (item d) from previous assignments may pose challenges. They argue that the nature of such engagements often demands a high-level of confidentiality to preserve the effectiveness of the assessments and that disclosing specific details about prior assignments could compromise the anonymity and security of the clients involved. Other members of the SGs are of the view that the introduction of TLPT as a standard requirement for qualifying FEs will necessarily involve a period of 'capacity-building' to ensure that adequate pools of experienced professional personnel are available.

From a practical point of view, the SGs note that it would be useful to include in the RTS a list of approved certifications for specific roles.

Q8. Do you think that the specified number of years of experience for threat intelligence providers and external testers 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.

The proposal for threat intelligence providers and external testers to have at least 5 years' experience is aligned with the TIBER-EU framework and could therefore serve as a useful point of departure. Some members of the SGs observe, however, that FEs should be provided with some more optionality, based on internal risk-assessments (see Q7. above).

In the longer run, the SGs suggest that it may be advisable to develop a framework for the accreditation of testers to ensure a minimum standard for providing and conducting relevant services, similar to the approach taken, e.g., by the Bank of England.

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

The SGs consider the proposed process generally appropriate. The SGs would like to highlight a few areas for improvement as follows:

- Paragraph 42 refers to the TLPT authority to issue an attestation in relation to 'critical systems in scope of testing'. This term does not exist either in the regulation text of DORA, nor anywhere else in the draft RTS and may need further clarification.

- The draft RTS assigns approval and validation tasks to the TLPT authority as part of the TLPT testing process, both ex-ante and for any changes to the TLPT as they occur. The latter may be impractical and the process should allow for greater flexibility, for example by pre-agreeing under what circumstances or scenarios the TLPT authority might only be notified of changes to the 'red team' test plan, without a need for formal approval. A notification procedure instead of an approval procedure may also be more practical in the case of pre-agreed or ad-hoc 'leg-ups'. Similarly, in the event that the testing activities are detected by any staff member of the FE or its ICT TPP, notification of, instead of validation by the TLPT authority may be more practical in order for the testing process to continue without undue delay.

- In general, the proposed timeframes appear appropriate. There may, however, be circumstances where timeframes would need a certain level of flexibility.

- The RTS requires the active red teaming test to be a minimum of 12 weeks. This should be understood as a default but exceptions should be possible, for instance, when a test exercise achieved its testing objectives in a shorter period of time, as demonstrated by the relevant protocols. Based on practical experience with TLPT, some members of the SG are of the opinion that a test period of six weeks (two weeks of active testing per each scenario) is typically sufficient to achieve the objectives of the test and, at the same time, help reduce TLPT test costs for FEs. Other members of the SG note that the TIBER-EU standard recommends a minimum duration of the 'red team' testing cycle of ten to twelve weeks. They note that TLPT should be mirroring a real-life scenario as closely as possible and undue time pressure, by compressing the time available to 'red team' testers, could render the exercise altogether meaningless.

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

The requirements for pooled testing lacks detail and present significant practical challenges for FEs, regulators and ICT TPPs. In the absence of guidance under the TIBER-EU framework in relation to pooled testing, it may be advisable to delay the use of pooled testing until such guidance is published. Pooled testing is not common practice across the financial sector yet and significant uncertainty remains concerning any attempts that have been made by TPPs to run such tests thus far. Once suitable guidelines are available pooled testing could be particularly relevant for FEs within the same group sharing critical business functions provided by an internally shared IT provider.

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.

The draft RTS requires several controls related to the use of internal testers. While the SGs agree with the controls listed, some of members consider certain requirements to be too prescriptive and argue that they introduce unnecessary burden and duplication. They suggest, in particular, that items (a.i.) and (a.iii.) of Article 11(1) are usually covered by the job descriptions, and assessed during the recruitment process for internal testers and should therefore be removed.

The SGs note that the draft RTS requires all members of the test team to be employed by the FE or an ICT TPP for the preceding two years. The draft RTS does not currently set out a rationale for this requirement, such as, presumably, the need for internal testers to be familiar with the infrastructure subject to testing. The SGs would welcome a more detailed explanation of that reasoning.

Furthermore, some members of the SG are of the view that some scenarios for 'red team' testing may not need a large team and suggest that a minimum number of two members should be deemed sufficient.

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

The draft RTS does not include information concerning the scope of a TLPT should it entail multiple TLPT authorities. There is a risk that the involvement of multiple TLPT authorities could lead to longer and more complicated testing. It would be advisable to incorporate procedural safeguards to ensure that the involvement of multiple TLPT authorities does not result in any material and unwarranted changes to its scope. The FE should still be allowed to respond to any scope to ensure the test remains rational to their operations across Member States. Most FEs in-scope of DORA TLPT tend to have centralised security teams who operate across all Member States and use the same set of ICT systems and controls. Adding applications on the basis that they are in use in a particular Member State would likely produce little in terms of incremental insights but would most probably result in added complication and difficulty in administering the test.

The draft RTS supports mutual recognition on the basis of three criteria: testing of critical or important functions, use of internal testers, and implementation of the TLPT as a pooled test. The SGs are of the view that these should not be the only criteria to be considered for recognition as there are other, equally important factors for recognition, e.g. whether the TLPT was carried out on common ICT systems and targeting the defensive teams that are involved in the FE's actual operations in the respective Member States. Art. 12(5) may be amended to reflect this criterion.

In addition, the report referred to in Article 26(6) and reflected in Annex VII should provide sufficient information to adequately inform a decision on mutual recognition.

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.

No further comments.

This advice will be published on the websites of the European Supervisory Authorities.

Adopted on 10 March 2024

[signed]	[signed]	[signed]	[signed]
Rim Ayadi Chair Banking Stakeholder Group	Michaela Koller Chair Insurance and Reinsurance Stakeholder Group	Veerle Colaert Chair Securities and Markets Stakeholder Group	Christian Stiefmueller Rapporteur