Contribution ID: 85a4c97c-a988-4ff1-83a5-07a061a9e7cb
Date: 04/03/2024 15:20:47

Public consultation on draft regulatory technical standards on specifying elements related to threat led penetration tests

Fields marked with * are mandatory.

Introduction

The European Supervisory Authorities (EBA, EIOPA and ESMA) have published the second batch of Consultation Papers on the mandates stemming from the Digital Operational Resilience Act (DORA) with the aim to collect market participants' feedback on the proposed Draft Regulatory Technical Standards on elements related to threat-led penetration tests.

Market participants are invited to provide their feedback to the draft technical standards by responding to the questions presented in this consultation paper by 4 March 2024. The feedback received will be taken into account in the finalisation of the draft technical standards, which are due to be submitted to the European Commission by 17 July 2024.

Comments are most helpful if they:

- respond to the questions stated;
- indicate the specific point to which a comment relates;
- contain a clear rationale; provide evidence (including relevant data, where applicable) to support the views expressed;
- reflect a cross-sectoral (banking, insurance, markets and securities) approach, to the extent possible; and
- describe any alternative approaches the ESAs could consider.

To submit your comments, please click on the blue "Submit" button in the last part of the present survey. Please note that comments submitted after 4 March 2024 or submitted via other means may not be processed.

Please clearly express in the consultation form if you wish your comments to be published or to be treated as confidential.

A confidential response may be requested from the ESAs in accordance with the ESAs' rules on public access to documents. We may consult you if we receive such a request. Any decision we make not to

disclose the response is reviewable by the ESAs' Boards of Appeal and the European Ombudsman.

The protection of individuals with regard to the processing of personal data by the ESAs is based on Regulation (EU) 1725/2018 of the European Parliament and of the Council of 23 October 2018. Further information on data protection can be found under the Legal notice section of the ESA websites.

General Information on the Respondent

* Name of the reporting stakeholder

European Association of Public Banks

Legal Entity Identifier (LEI), if available

* Type of Reporting Organisation

- ( ) ICT Third-party Service Provider
- ( ) Financial Entity
- (•) Industry Association/Federation
- ( ) Consumer Protection Association
- ( ) Competent Authority
- ( ) Other

* Financial sector

- [x] Banking and payments
- [ ] Insurance
- [ ] Markets and securities
- [ ] Other

* Jurisdiction of establishment

Belgium

* Geographic scope of business

- ( ) EU domestic
- (•) EU cross-border
- ( ) Third country
- ( ) World-wide (EU and third country)

* Name of Point of Contact

Mathilde Pradeau

* Email address of point of contact

mathilde.pradeau@eapb.eu

* Please provide your explicit consent for the publication of your response

- (●) Yes, publish my response
- ( ) No, please treat my response as confidential

Questions

General drafting principles

* Question 1. Do you agree with the proposed cross-sectoral approach?

- (●) Yes
- ( ) No

Please provide additional comments (if any)

* Question 2. Do you agree with the proposed approach on proportionality?

- ( ) Yes
- (●) No

* Please provide detailed justifications and alternative wording as needed

No. According to Article 26 (8) subparagraph 3 DORA, the FEs that must carry out a TLPT are identified by the authorities. This indicates that institutions do not have to carry out a TLPT if they are not appointed. Article 2 para. 1 RTS indicates in contradiction to this that certain institutions are obliged and the task of the authority is to exclude institutions from these.
In accordance with Article 26 (8) subparagraph 3 DORA, we therefore propose that the wording in Article 1 (1) "Competent authorities shall require financial undertakings..." be replaced by "Competent authorities shall identify financial undertakings...". to "Competent authorities shall identify financial undertakings...and notify them bilaterally".
The operational structure of ICT systems for FEs operating in several Member States is not taken into account. In most cases, mature FEs with multiple entities and branches will use the same ICT systems with central control and cybersecurity departments managing their internal testing programs. A TLPT authority of a Member State could identify a FE based on a "specific characteristic" that includes exactly the same ICT systems and control procedures tested by another TLPT authority. The argument used in the RTS for the principle of proportionality does not relate to the operational practices of financial entities operating in the EU.
We therefore propose: The IT structure of the respective FE - especially if it is active in several Member States - as well as TLPT tests already carried out are taken into account in the identification as well as in the implementation (with coordination between the authorities).

Approah on the identification of financial entities required to perform TLPT

* Question 3. Do you agree with the two-layered approach proposed to identify financial entities required to perform TLPT?

- (●) Yes
- ( ) No

Please provide additional comments (if any)

We agree with the two layered approach. That having said, the criteria for including other financial entities provided by Article 2(3) interacts with the criteria for resolution purposes. It would make sense to clarify that institutions which are subject to simplified obligations (in accordance with Article 11 of EU 806/2014) and for which the preferred resolution strategy in normal insolvency are explicitly excluded from the option to include as the result of the assessment here should be aligned with the result of the assessment for resolution.
The refers to "Payment institutions, exceeding in each of the previous two financial years EUR 120 billion of total value of payment transactions". Even when interpreting Art. 5 No. 5 of Directive (EU) 2015/2366, it is not clear whether the sum of incoming and outgoing payments or only one of them is to be considered. It is also questionable whether securities trading is included.

* Question 4. 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?

- (●) Yes
- ( ) No

Please provide additional comments (if any)

Approach on the testing: scope, methodology, conclusion

* Question 5. Do you consider that the RTS should include additional aspects of the TIBER-EU process?

- ( ) Yes
- (●) No

Please provide additional comments (if any)

* Question 6. Do you agree with the approach followed for financial entities to assess the risks stemming from the conduct of testing by means of TLPT?

- ( ) Yes
- (●) No

* Please provide detailed justifications and alternative wording as needed

No, we believe that risk management is not sufficiently considered. ICT Third-Party providers should be responsible for managing possible negative effects of the test towards other customers. FE's control teams can only manage the FE's risk as they have no sufficient insight, influence nor mandate to manage that of other customers and/or suppliers. Also, we are unsure of the added value of including third-party infrastructure within testing. It could lead to less transparency due to additional safeguards that need to be build in to account for all risks. FE's have developed other means to identify potential vulnerabilities within third-party providers like risk assessments, due diligence questionnaires etc. that can sufficiently and appropriately manage the possibly exposed risks.

* Question 7. Do you consider the proposed additional requirements for external testers and threat intelligence providers are appropriate?

- (●) Yes
- ( ) No

Please provide additional comments (if any)

In general we agree, however we note that the proposed criteria limited the market for external testers extensively. This can pose a risk for timely and appropriate testing as FE's will simply not be able to source relevant parties and in our view competent other parties are excluded. FE's can get overly reliant on a handful of market-parties this way that also benefit from gaining extensive and dep insight into financial entities way of working and infrastructure further strengthen their position.
Especially 2.c & 2.d exclude companies due to the requirement of previous engagements while they could have sufficiently skilled employees. We propose more flexibility to assess based on employees skills where previous engagements of the company is not available. 2.e.i should be more flexible to also allow threat intelligence providers with no experience in financial industry but similar experience in other industries. 2.f.ii should be not mandatory but optional as the focus lies on digital resilience and physical penetration is only a very small and particular part of that from a threat perspective.
Overall we strongly feel that more flexibility is needed in the criteria to allow FE's and CA's to select from a broader pool of external testers as the current criteria will lead to a situation where TLPT can't be appropriately and timely executed in each member state by each FE.

* Question 8. 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?

- ( ) Yes
- (●) No

* Please provide detailed justifications and alternative wording as needed

No. The target of 5 years of professional experience is critical.
The specification of professional experience in annual figures in no way reflects the personal or professional suitability that a test person must demonstrate in order to carry out realistic TLPT in productive systems of FE's. The test person must be able to demonstrate experience in at least several comparable projects that justifies their deployment in an adequate role for the upcoming TLPT.
Proposal: Delete Art. 5.2 e and f. Instead, the points can be supplemented in an annex with possible quality criteria. In the long term, certificates for testers would be suitable.
For clarification, it should be stated in Article 5 that the references are required at the level of the personnel and not at the level of the service provider, in order to avoid a situation where a newly established company cannot be commissioned because it lacks references but consists of experienced personnel with the required references.

* Question 9. Do you consider the proposed testing process is appropriate?

- ○ Yes
- ◉ No

* Please provide detailed justifications and alternative wording as needed

No.Art. 6: This must currently be completed within the specified 6 months of the preparation phase.
This could prevent FE's from ensuring proper budgeting and compliance with our procurement guidelines, especially when contracting suppliers that are not yet subject to a framework agreement with the FE's
Art. 9.4: Our experience in previous TIBER exercises shows that 4 weeks is not enough time for the blue team to thoroughly analyze the red teaming activities performed and write a detailed report. Proposal: The blue team is given at least 12 weeks to prepare a detailed report that can be used for planning remedial actions.
Art. 9.7: Experience has shown that 12 weeks is too short for the preparation of the finding report. We recommend at least 16 weeks.
Art. 10.1: The required 16 weeks for the completion of the remediation planning are generally appropriate. However, the reference point of 16 weeks is too early if a Purple Team is used, as sufficient time must be available for coordination and the definition of effective and realistic measures.
The number of scenarios and targets should never be specified independently of the results of the TI phase. We suggest that certain scenarios be weighted higher depending on the results of the TI phase and that other scenarios be made optional as a result.

* Question 10. Do you consider the proposed requirements for pooled testing are appropriate?

- ○ Yes
- ◉ No

* Please provide detailed justifications and alternative wording as needed

No. As combined and pooled tests are very complex, more information and clarification is needed to fully understand how these tests can be conducted efficiently and risk-free. It is unclear how a pooled test is initiated if the FEs are unaware of each other's commitment to TLPTs and use the same ICT TPP. It should be specified in more detail how the pooled tests are to be organized, in particular with regard to the time sequence. To this end, the responsible TLPT authorities must coordinate with each other and with the FE's and ICT-TPPs.

Approach on the use of internal testers

* Question 11. Do you agree with the proposed requirements on the use of internal testers?

- ○ Yes
- ◉ No

* Please provide detailed justifications and alternative wording as needed

No, Article 5(2) stipulates exact requirements for external testers whereas such requirements for internal testers are absent, Article 11(1)a stipulates that the FE shall establish a definition and implementation of a policy for the management of internal testers in a TLPT. This might however lead to a large discrepancy between requirements for external testers and internal testers. We are surprised to see more stringent requirements on insider screening for internal staff, compared to external staff. We expect the FE to set more stringent requirements to internal staff by applying a policy for internal staff on top of the DORA requirements, including technological experience etc.

Approach on cooperation

* Question 12. Do you consider the proposed requirements on supervisory cooperation are appropriate?

- ◉ Yes
- ○ No

Please provide additional comments (if any)

Final comments

Question 13. Do you have any other comment or suggestion to make in relation to the proposed draft RTS?

The RTS describes the (not limitative) information which informs the ICT Maturity of a Financial Institution. However it is not clear how this maturity level will be decided on. This poses a risk for possible subjective interpretation of the term ‘’maturity’’ over one or more NCA’s/ESA’s. A common framework with objective criteria to establish a level of ICT maturity would be helpful and possibly prevent entities in Country A to fall under TLPT while similar entities in country B are not selected by their NCA. It is also unclear what the timeline will be for FE’s which have already performed TIBER tests recently. DORA requires TLPT at least every 3 years, but what happens when an FE has already performed advanced testing in for example 2024, is the next expected test then 2027 latest or all previous test not accepted? We suggest to amend the text to clarify that FE’s can rely on at least the last TLPT test performed and count from there on.

Article 8: In Article 8 sections 5., 6., 8., 9., and 10. it is unclear who is meant by the “TLPT authority” (ECB or Test Manager). A better wording would be to use the definition “test manager” in this context.

Article 4 section 2.a.: The list of groups receiving access to parts of the information should be extended. Multiple processes to organize and finance a TLPT require members of the financial entity that are not part of the control team or management body. We recommend to change the requirement in a form so that it allows for individual exceptions under supervision of the test managers. General introduction (page 21) section (18): The examples for possible leg-ups should be clearly marked as examples, because not every control team can provide access to any ICT system for the testers.

Annex V: It is unclear how section (b) d. belongs in a red team report. We suggest deleting this requirement.

Contact

Contact Form