Contribution ID: 2278edb0-611b-4bec-bb0d-1d6b482405ed
Date: 04/03/2024 22:11:34

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

Electronic Money Association

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

Judth Crawford

* Email address of point of contact

judith.crawford@e-ma.org

* 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)

We support the adoption of a TLPT testing methodology that is technology and entity-agnostic. However, we would also encourage the ESAs to assess the benefits of the re-use of the information security testing frameworks that many financial service providers have established to comply with the requirements in the EBA Guidelines on ICT and security risk management (EBA/GL/2019/04). We perceive that some of the outputs of existing information security testing processes that financial service providers have established could be inputs to the TLPT that will be carried out to comply with DORA requirements.

* Question 2. Do you agree with the proposed approach on proportionality?
  - (●) Yes
  - ( ) No

Please provide additional comments (if any)

We support the application of the proportionality principle in the criteria that are used to identify FEs that required to perform TLPT (degree of systemic importance, ICT maturity). It would be helpful if the ESAs clarified the threshold of ICT maturity that must be exhibited by FEs that are required to perform TLPT.

Additionally, we encourage the ESAs to consider the application of proportionality to the requirements associated with the testing process reflecting the varying size/profile and ICT resources of financial entities that may be required to complete TLPT under DORA. We list proposed changes to the testing process detailed in the RTS in our response to Question 9 below.

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 detailed justifications and alternative wording as needed

We are concerned that the two-layered approach detailed in Art.2 of the RTS includes a number of ICT-risk related factors that are briefly outlined at a high level (risk profile, threat landscape, ICT maturity). The interpretation of such ICT risk factors may well diverge across TLPT Authorities in member states leading to inconsistencies in the designation of FEs that are required to take on the significant operational overhead of completing TLPT. We encourage the ESAs to review all the ICT related risk factors listed in Art. 2(3) of the draft RTS to facilitate consistent interpretation and application by TLPT authorities.

Additionally, it is not clear why some ICT service arrangements are identified as ICT risk related factors that could prompt a TLPT Authority to require a FE to perform TLPT. Specifically,

The degree of dependence of critical or important functions or their supporting functions of the financial entity on ICT systems and processes

The complexity of the ICT architecture of the financial entity

The ICT services and functions supported by ICT third-party service providers, the quantity and type of contractual arrangements with ICT third-party service providers or ICT intra-group service providers

Whether the financial entity is part of a group active in the financial sector at Union or national level and using common ICT systems.

It is quite common for EU FEs of varying sizes to use ICT systems/services - provided by external or intragroup service providers - to support Critical/Important business functions. These FEs already manage the relevant ICT risks (including outsourcing risks) in their risk management framework and are required to have in place an information security testing framework . In this context, it is not obvious that the existence of such arrangements gives rise to an elevated ICT-related risk. We propose that the ESAs remove the ICT service arrangements listed above from the list of ICT risk related factors listed in Art. 2(3) of the draft RTS.

* 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)

We support the quantitative criteria listed in Art. 2(1) of the draft RTS to identify entities offering core financial services that will be required to perform TLPT.

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)

We believe that the ESAs should continue to use a tailored approach to identifying elements of the TIBER EU framework that is reused to meet the Advanced testing requirement in DORA reflecting the (i) constituency that will be required to complete TLPT under the Regulation (compared to the voluntary TIBER-EU framework) and (ii) the mandatory nature of the advanced testing requirements in DORA.

In this context, we do not support the inclusion of additional aspects of the TIBER-EU framework in the RTS; we would also encourage the ESAs to review the mandatory inclusion of Purple team meetings/workshops in the TLPT testing framework described in the RTS.

* 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

Yes and no.

We appreciate that the risk management responsibility for the TLPT process will reside with the FE undergoing such testing. We also want to point out the limited access to TLPT (including TIBER -EU) risk management expertise in the EU financial services ecosystem. In this context, we encourage the ESAs to consider (i) The use of parent/group TLPT risk management expertise by the control (white) team of the FE under testing and (ii) The role of the TLPT cyber team(s) as a source of TLPT risk management guidance for the FEs that are undergoing TLPT.

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

- ○ Yes
- ◉ No

* Please provide detailed justifications and alternative wording or thresholds as needed

In the context of the already constrained access to TIBER-EU testing expertise that is experienced by financial entities undergoing TIBER-EU testing, we would propose that the ESAs requirements on internal /external testers focus on (i) The establishment of a certification scheme that certifies the expertise, knowledge base of individuals participating in Red team testing activities and (ii) The scope of recent involvement of individual Red team members in conducting TLPT activities rather than years of experience. This approach can potentially help grow the availability of knowledgeable, credible tester resource that can be used by FEs to support their TLPT activities.

* 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

Per our earlier response (to Question 7 above), we perceive that the number of years of experience in threat intelligence (TI) and red-team testing (RTT) activities should not be the only qualifying factor for TI and RTT team members.

The scope of recent involvement of individual team members in relevant TI/RTT activities is also a valid proxy for competence/knowledge that should be considered. We propose a minimum of five (5) completed TLPT-related engagements for TI/RTT team leads and two (2) for team members. We would also suggest that FEs are required to collect previous client references from at least three (3) previous TLPT assignments for both TIPs and RTT providers rather than the 5 references for the latter suggested in Art. 5(2)(d) of the draft RTS. Our suggestions aim to facilitate a growth in the number of entities that can offer TIP and RTT services in support of the TLPT processes of EU financial entities.

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

- ○ Yes
- ◉ No

* Please provide detailed justifications and alternative wording as needed

The proposed scope and duration (>10 months) of the testing process will have a significant impact on the ICT, human and financial resources of FEs that are required to complete such testing. We note that the number, size & profile of FEs that may be required to complete TLPT under DORA is likely to differ from the few, large Credit Institutions that have completed optional TIBER-EU testing, so far.

Additionally, we note the high degree of involvement of TLPT Cyber Teams (TLCs) in the TLPT of any FE that is required to complete such testing (reviewing potential tester engagements, approving scoping documents and test plans, reviewing test summary reports etc). We are concerned that TLPT Authorities may not be able to establish/maintain the TLCs that are required to support TLPT exercises run concurrently by a number of FEs.

In the context of the above, we would encourage the ESAs to adopt a risk-based approach in the definition of the Testing process that (i) Reflects the growing numbers of FEs that may be required to perform TLPT under DORA, (ii) Acknowledges the significant cost/resource overheads associated with a multi-month TLPT effort and (iii) Considers the ability of TLPT Authorities to support high-frequency interactions with concurrent TLPT projects.

Following our comments above, we propose that the ESAs consider:

A decrease of the minimum duration for the Active Red Team testing phase to 8 weeks (rather than the 12 weeks referenced in Art. 8(5))

The removal of the replay and purple team testing exercise requirements from Art. 9 of the RTS.

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

- ◉ Yes
- ○ No

Please provide additional comments (if any)

We offer no comment on the proposed requirements for pooled CLPT.

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 additional comments (if any)

We support the definition of requirements to ensure that Internal Testers - supporting the TLPT activities of FEs - possess the necessary skills, experience, expertise and managerial independence to act as a credible Red Team testing resource. We are also aware of the limited access to specialist Red Team testing resources that many EU financial service providers are encountering, at present. In this context, the mandatory minimum 2-year employment history for Internal Testers in Art.11 of the draft RTS reads as an unwarranted obstacle for FEs that seek to build up their internal understanding of TLPT services and to establish internal tester teams.

We propose that the RTS focuses on the skills, knowledge, experience (evidenced through individual tester certification and involvement in TLPT red team testing engagements) of Internal Tester team members rather than on an arbitrary minimum employment requirement before an individual can join an Internal Tester team.

Approach on cooperation

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

- (●) Yes
- ( ) No

Please provide additional comments (if any)

We support the proposed requirements on supervisory cooperation between TLPT Authorities. We encourage the ESAs to ensure that TLPT attestations issued by a TLPT Authority are mutually recognised across the Union.

Final comments

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

We seek further clarity on the rationale for the introduction of a mandatory requirement to include Purple Teaming as part of the Closure Phase of the Testing process in the Art. 9(4) of the draft RTS. This is an optional requirement for the TIBER-EU framework and its mandatory inclusion in the TLPT carried out by in-scope entities will further increase the cost/effort and impact on their resources.

We are concerned about the preparedness of TLPT Authorities to adopt the governance structure changes identified in the early part of the RTS and to stand up the required number of TLPT Cyber Teams (TCTs) with appropriate levels of TLPT expertise to support multiple FEs that raise operational questions in the course of performing TLPT activities. We encourage the ESAs to work with the designated TLPT Authorities to ensure that the availability of TCTs does not inhibit the completion of TLPT activities by in-scope financial entities.

Contact

Contact Form