Contribution ID: 31abd620-db74-4025-86b7-b25469d42c20
Date: 04/03/2024 13:27:49

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

Dutch Federation of Pension Funds

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

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

* If other, please specify

Pensions

* Jurisdiction of establishment

Netherlands

* Geographic scope of business

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

* Name of Point of Contact

Martin van Rossum

* Email address of point of contact

rossum@pensioenfederatie.nl

* 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 would like to highlight that the IORPs carry lower risks than other financial entities. Being at the buy-side of the financial sector, disruptions have a low impact on the financial sector; the systemic character of IORPs is low; and considering the monthly administration cycle, the ICT risks of pension administration are low throughout most of the month. This should lead to a more cautious and proportionate approach towards TLPT for IORPs.

Moreover, some scenarios that are relevant for one sector are irrelevant for another. Scenarios should be tailored to the relevant risks in a particular sector.

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

- ( ) Yes
- (●) No

* Please provide detailed justifications and alternative wording as needed

Article 2 of the RTS on TLPT allows TLPT authorities to require certain financial entities to perform TLPT, on the basis of a number of criteria. Considering that pension policy is a national competence and the IORP II Directive prescribes minimum harmonization, IORPs vary widely between Member States. That makes it hard to specify EU criteria for IOPRs on the application of TLPT. National TLPT authorities seem better placed to us to determine whether IORPs and their service providers have to perform TLPT.

We think there should be stronger proportionality considerations in Article 2(3) as well as Section II of the RTS. We note that Dutch IORPs, being at the end of the financial service value chain, carry a very low degree of systemic importance. They do not deliver B2C financial services and therefore pose very low risks to the continuity of core financial services.

Preparation for TLPT takes considerable time. TLPT authorities should allow enough time between the assessment that a pension is required to perform TLPT and the first testing.

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. It provides clarity that types of financial entities with a systemic character have to perform TLPT, while leaving the assessment for other entities up to TLPT authorities.

* 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 additional comments (if any)

* 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

We would like to highlight that the draft RTS is going beyond the level 1 empowerment which does not give a mandate to ESAs as regards criteria for external testers.

Risk management for the TLPT is an important topic. Article 5 prescribes that the control teams takes measures to manage the risks and shall ensure that:
- the threat intelligence provider provides at least three references from previous assignments related to intelligence-led red team tests (under c); and
- the external testers provide at least five references from previous assignments related to intelligence-led red team tests (under d).

We expect this to prove problematic. Companies that are subject to TLPT (or similar testing) often do not wish to be named as a company that is subject to testing, given the implications it can have for the reputation of a company.

Furthermore, the demand for a minimum amount of references creates a barrier for entry. That makes it hard to enter the market and could strongly compress the market of threat intelligence provision. The ESAs should consider how conditions for threat intelligence providers would affect competition and consequently consumer protection.

Rather than taking a rules-based approach, prescribing absolute minimum amounts of references and years of experience, a more principle-based approach should be taken, in which financial entities assess whether the threat intelligence provider is capable and has relevant experience.

* 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

The number of years of experience for testers seems arbitrary and very prescriptive. A staff member of the threat intelligence provider might have 4.5 years of experience instead of 5 years, and therefore not qualify according to the RTS. It might also limit the number of threat intelligence providers or external testers while not necessarily increasing the quality of said parties.

We suggest to approach this more principle based and to require for 'a proven track record' for external testers and threat intelligence providers.

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

- ( ) Yes
- (•) No

* Please provide detailed justifications and alternative wording as needed

Article 4(2) under c of the RTS states that the control team is informed of any detection of the TLPT by staff members of the financial entity or of its third-party service providers, where relevant, and the control team contains the escalation of the resulting incident response, where needed. This seems to be counterproductive. Besides the TLPT team, nobody within the company (the tested entity) knows about an ongoing TLPT. The control team cannot be informed if staff members have detected a TLPT. That would imply that every suspicious activity needs to be reported to the TLPT team, even when that is not part of a TLPT. This would result in an extra reporting line and it would also imply that people within the organization know who is part of the control team (which is not always in function).

We note that testing is only feasible with direct contracting parties. Financial entities should not be required to test further down the subcontracting chain. The RTS should clarify this.

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

- ( ) Yes
- (•) No

* Please provide detailed justifications and alternative wording as needed

The processes for pooled testing is not adequately described in the RTS. That creates legal uncertainties. Principles for cooperation between financial entities and their interaction with the party being tested could help to give clarity to all parties involved. That would facilitate more frequent use of pooled testing, which is more efficient for all parties involved.

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

The criteria for in-house testers are too restrictive and will make it difficult to use in-house testers. As the market for external testers is very small, this is likely to constitute a major practical obstacle to the implementation of TLPTs.

Less granularity and more flexibility should be offered. The criteria set at level 1 – requiring using testers that are certified or adhere to a code of conduct or an ethical framework are sufficient and more appropriate. At the very least, the requirement to have been with the company for two years should be limited to a single member of the testing team in Article 11 (1) (a) (ii).

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?

Not included in the RTS is the obligation for the TLPT authority to set up ‘Chinese Walls’ (barriers to information) between the internal TLPT team of the TLPT authority and its regular supervisory teams (e.g. prudential and market conduct supervision). The findings of the TLPT authority should not result in enforcement by the ‘regular’ supervisory team of the TLPT authority or other NCAs. We suggest adding the requirement of Chinese walls within the TLPT authority to either article 2 or 3 of the RTS.

The TIBER-NL framework prescribes that the testing authority gets informed about preparation and performance of TIBER testing. The authority can only access the documentation at the financial entity’s premises, to prevent that this very sensitive information is concentrated at one point. The DORA RTS require to provide the TLPT authority with this information. It is questionable if this is wise.

We find it inappropriate that the TLPT Authorities are tasked “to organise” and “to lead” the TLPT. They cannot both lead a test and evaluate the results of the test impartially. This approach is not aligned with Article 26 and Article 27 of the Level 1 text.

Contact

Contact Form