Contribution ID: d630c65e-a816-4731-a9d9-0f3da396853a
Date: 01/03/2024 14:44:12

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

Deutsche Boerse Group

Legal Entity Identifier (LEI), if available

529900G3SW56SHYNPR95

* 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
- [x] Markets and securities
- [ ] Other

* Jurisdiction of establishment

Germany

* Geographic scope of business

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

* Name of Point of Contact

sujata.wirsching@deutsche-boerse.com

* Email address of point of contact

sujata-wirsching@deutsche-boerse.com

* 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)

No comment.

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

* Please provide detailed justifications and alternative wording as needed

In general, we agree with the proposed approach on proportionality. However, concerning FMI, we do not see that the proportionality approach is fully respected.
We also would like to emphasise that size should not be the main metric when determining cybersecurity requirements. Rather entities having similar risk profiles should be subject to similar requirements.

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)

No comment.

* 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)

No comment.

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 suggestions

We consider the RTS to sufficiently reflect the main aspects of TIBER-EU. However, we feel that the metrics for external testers and threat intelligence providers are likely to limit the availability of testers. For a more detailed answer please see below.

* 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)

We consider the RTS to sufficiently reflect the main aspects of TIBER-EU. However, we feel that the metrics for external testers and threat intelligence providers are likely to limit the availability of testers. For a more detailed answer see Q7b.

* 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 point out that the requirements for external testers are very comprehensive and may not be fully controlled in practice. TLPTs are usually carried out by a large team, and it is difficult to verify the experience of all testers. Or there may be a lack of certificates and, thus, a limited availability of eligible testers. Furthermore, not every provider of such tests is likely to have insurance that covers TLPT activities, as the risk is very high, and costs could quickly exceed the value of the company. It is important that the company carrying out the test has a good reputation and good references. Those are the most important factors listed in Article 5, from our point of view.

* 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

In our view, the specified number of years of experience for external testers and threat intelligence providers assigned to the TLPT (as provided in Article 5(2) points (e) and (f)) is not an entirely appropriate measure to evaluate the staff's knowledge and skills and does not necessarily reflect their overall suitability and reputability. In fact, we would like to highlight that the proposed number of years of experience appears as quite stringent and restrictive considering the general scarcity of such resources in the market.
To provide more flexibility, we would suggest replacing the "number of years of experience" criteria with "sufficient expertise", as we strongly believe that financial entities shall be able to decide, after conducting a thorough selection process and assessment, if the external testers and the staff of the threat intelligence provider assigned to the TLPT have sufficient and appropriate qualification and therefore satisfy the expertise requirement.

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

- Yes
- No

* Please provide detailed justifications and alternative wording as needed

We would like to raise key concerns regarding the proposed process on the performance of threat led penetration tests, as provided in Chapter III of this RTS.
Firstly, related to the testing environment – we believe that conducting the tests on live production systems presents unacceptable risks with potential negative impacts not only for the trading venues and their trading systems, but also for trading participants and financial entities depending on continuous price information.
In general, financial entities and particularly trading venues are required to "ensure a strict separation between the testing and the production environment or permit testing only out of trading hours" (i.e., RTS specifying organisational requirements of trading venues under MiFID II). As the threat led penetration tests are required to be conducted on live production systems already under Article 26 of DORA, we believe that financial entities must at least be granted more flexibility and discretion to determine the moment and time deemed most appropriate to perform the tests – for instance during non-critical/core operating hours. This is an essential aspect to consider in order to minimise the potential for risks and avoid significant disturbances and negative impacts on the business and operations of trading venues.
Secondly, the proposed RTS stipulates that testing process shall be conducted for a duration of 12 weeks. We would like to point out that, due to this set duration, the performance of these tests will become highly complex in case multiple trading venues, that are running on the same trading system, are required to perform the testing process by the TLPT authority at the same time. From our perspective, it would be highly beneficial for financial entities to be able to cluster these tests above the group level, thus allowing entities that use common trading systems or same ICT service providers to conduct the tests jointly. This would reduce complexity and enhance efficiency.
We would also we call for more discretion on the timeframes. Specifically, when it comes to the Closure phase. Here we would suggest a less stringent timeline or at least allow more flexibility for the provision of the intermediate reports / steps as especially the members of the blue team have continues BAU activities and might therefore need more time for activities they are responsible for / involved in.

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

- Yes

- [x] No

* Please provide detailed justifications and alternative wording as needed

While we overall agree with the proposed requirements for pooled testing, some aspects are lacking clarity from our perspective.
In order to reduce complexity and ensure more flexibility, we believe that financial entities not belonging to the same group shall be able and allowed to conduct pooled testing jointly, as long as these entities are using common ICT systems or same ICT service providers. To enhance clarity, we suggest explicitly including such a provision in Article 12 of the draft RTS.
In addition, it should be clarified how it can be assured that a pooled test performed by an ICT service provider includes all institutes for which this ICT service provider would be part of their TLPT scope. It should be avoided that an ICT service provider which has a large number of clients falling under the DORA TLPT requirement is continuously approached by individual or groups of respective clients with the request to perform pooled testing.

Approach on the use of internal testers

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

- [ ] Yes
- [x] No

* Please provide detailed justifications and alternative wording as needed

We understand the intention of the regulators to include two years of prior employment for internal testers. However, this creates a discrepancy between the requirements for external and internal testers. We believe the requirements should align as the internal knowledge the internal testers would gain does not provide an additional value when simulating an attack.
In addition, this requirement significantly impacts the practicality to use internal testers. The reason for this is, that with a staff turnover, as it is common in the industry, it would be impossible for an institute to ensure that internally set up team fulfills these requirements.

Approach on cooperation

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

- [x] Yes
- [ ] No

Please provide additional comments (if any)

No comment.

Final comments

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

We would ask to clarify whether an institute that has successfully performed threat led penetration test (TLPT) itself, does therefore not need to be included in the individual TLPTs of their customer. If this would not be the case, it would lead to a very high burden on several institutes, due to the level of interconnection in the financial service industry. Especially trading venues, central securities depositories, etc. could, due to their role in the market, be in scope of the TLPTs of a very high number of clients, making it not feasible to participate in these individual tests. The additional value of including institutes who already performed an TLPT would at the same time be limited, as the relevant infrastructure supporting ICT services would be covered by their own tests.

Contact

Contact Form