German Banking Industry Committee

Die Deutsche Kreditwirtschaft

Comments

Public consultation on draft RTS on specifying elements related to threat led penetration tests (JC 2023-72)

Lobby Register No R001459
EU Transparency Register No 52646912360-95

Contact:
Frank Trojahn
Telephone: +49 30 20225-5513
E-mail: frank.trojahn@dsgv.de

Berlin, 2024-02-27

Coordinator:
German Savings Banks Association
Charlottenstraße 47 | 10117 Berlin | Germany
Telephone: +49 30 20225-0
Telefax: +49 30 20225-250
www.die-deutsche-kreditwirtschaft.de

General drafting principles

Comments Public consultation on draft RTS on specifying elements related to threat led penetration tests (JC 2023-72)

Question 1. Do you agree with the proposed cross-sectoral approach?
No
We propose the following amendments to recital 19:
We are of the view that the TLPT authority may waive a purple team exercise for the purpose of the learning effect if the control team determines that the benefit to the financial institution is limited, provided that only minimal weaknesses were identified during the red team exercise.

Similarly, we propose to amend Article 9 (5) and 9 (6):
"Where limited vulnerabilities have been identified and the control team, blue team and testers consider that a purple team exercise would not provide a benefit to the financial institution, the control team may approach the TLPT authority to waive the mandatory conduct of a purple team exercise."

Question 2. Do you agree with the proposed approach on proportionality?
No
According to Article 26 (8) subparagraph 3 DORA, the FEs that must conduct 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 (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 changing the wording in Article 1 (1) "Competent authorities shall require financial institutions.." to ""Competent authorities shall identify financial institutions...and notify them bilaterally"".

The operational structure of ICT systems for financial undertakings operating in several Member States is not taken into account. In most cases, mature financial institutions 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 financial institution 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 institutions operating in the EU.

We therefore suggest: The IT structure of the respective financial institution - 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 authorities).

Question 3. Do you agree with the two-layered approach proposed to identify financial entities required to perform TLPT?
No
Art. 2.3 (a) and (b): The ICT risk-relevant factors (b) are formulated relatively openly. If these are used as independent criteria, then many financial companies are the focus of the TLPT. For example, the dependency of critical and important functions on ICT is always high. Therefore, a combination of factors from (a) "impact-related and systemic nature" and (b) "ICT risk-related factors" should always be used to determine the financial institutions affected. For example, the criteria could be categorized as low / medium / high, and only if the criteria in (a) and (b) are categorized as high should the financial institution be eligible for a TLPT.

Comments Public consultation on draft RTS on specifying elements related to threat led penetration tests (JC 2023-72)

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?
No
"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 the two is to be considered here. It is also questionable whether securities trading is included. We therefore ask for clarification as to which calculation basis is being used here.

We propose that outgoing payments initiated via the institution's clients be used.

Question 5. Do you consider that the RTS should include additional aspects of the TIBER-EU process?
No
The currently regulated scope basically takes into account all necessary framework conditions for the implementation of a TLPT. The inclusion of further aspects would make the cost-benefit ratio worse due to stricter rules.

Voluntary elements should be allowed, e.g. Purple Teaming (see question 1) should be optional - similar to TIBER. See also answer to Q1

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?
No
The special risk management requirements for tests with ICT third-party providers (not pooled) or pooled tests are not sufficiently taken into account. In both cases, the ICT TPP should be responsible for risks that the test has a negative impact on other customers or internal processes of the service provider. The financial institution's control team can only assess and manage the risks for its own organization.

The high number of tests performed across the EU may result in a financial institution being unable to award a contract in accordance with the prescribed criteria. We recommend giving the FE the option to postpone a TLPT in agreement with the TLPT authority if the financial institution is unable to establish a sufficient level of security to conduct the TLPT.

Proposed amendment:
Article 5 (2) (j):"If the control team is unable to procure external providers that meet the requirements of Article 5, it shall notify the TLPT authority and consider postponing the TLPT until the procurement guidelines can be met."

It is not clear from the RTS whether the same company can act as both a threat intelligence provider and an external tester for the TLPT. To reduce the complexity of the contract and the time required to complete a test, the external tester often also takes on the role of threat intelligence provider. This should be clarified in the RTS to ensure that this can remain common practice.

Comments Public consultation on draft RTS on specifying elements related to threat led penetration tests (JC 2023-72)

It is important that the institution's risk management is given the opportunity to challenge the TLPT scenarios. A TPLT authority may significantly increase the risk of a TLPT by proposing test scenarios that are broad or vague, or that do not relate to the real-world operation of an institution's ICT systems.

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

No

Very few providers currently meet all the criteria and therefore the market is very narrow. If a large number of financial institutions simultaneously search the market for testers with the desired profile, demand will significantly exceed supply. It is therefore questionable whether the expectations of timely fulfillment of the test plans can be met. The requirements for TIBER/DORA tests should therefore be reduced. At least for the period of the DORA introduction (ramp-up phase), the requirements should be suspended until enough service providers have been able to form teams with the desired profile. We suggest that the ESA or the authority responsible for TLPT consult with leading industry associations.

By restricting the market, a massive increase in the cost of TLPT is to be expected, so that the implementation of a high-quality TLPT will have a poor cost-benefit ratio. On the other hand, TLPTs are also at risk, as financial institutions may not be able to find a provider. The requirements will exclude many established threat intelligence and red team providers in Germany from implementing TLPTs. Requirements must be lowered to enable new companies to enter the market and to ensure that there is sufficient capacity in similar test environments.

Art. 5 (2) c. & d. These requirements could exclude new companies that have qualified employees but have not yet worked in their current company. We suggest that the experience of the employees of the test team is sufficient as a reference and not the company itself.

Suggestion to c. and d.: the provider of threat data or the external tests should provide suitable references that they or their employees have experience from previous assignments in connection with Red Teaming.

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?

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 aptitude that a test person must demonstrate in order to carry out realistic TLPT in productive systems of systemically relevant financial institutions. 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 newly established company not

being able to 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?
No
Art. 6: It is assumed that the procurement should also be completed within the specified 6 months of the preparatory phase. This could prevent us from ensuring proper budgeting and compliance with our procurement guidelines, especially if suppliers are to be engaged who are not yet under a framework agreement.

Art. 8: The timeframe of at least 12 weeks for the active testing phase of the red team is in principle reasonable. If a test agreed with the supervisory authority can be carried out in less time, this minimum should not unnecessarily prolong the test. We ask for clarification as to whether cooling-off phases or complete interruptions of one or more scenarios lead to an extension of the 12 weeks.

Art. 9.4: Our experience in previous TIBER-DE exercises shows that 4 weeks is not enough time for the blue team to thoroughly analyze the conducted red teaming activities and write a detailed report. We strongly suggest that the blue team be 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 there must be sufficient time for coordination and the definition of effective and realistic measures.

It seems that the number of scenarios and targets are given independently of the results of the TI phase. We propose 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?
No
As combined and pooled tests are very complex, more information and clarification is needed to fully understand how these tests can be performed efficiently and without risk.

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 and the ICT-TPP.

Question 11. Do you agree with the proposed requirements on the use of internal testers?
No
Policy for the management of internal testers: The consultation paper in 52(a) states that the financial institution must "define a policy for the management of internal testers in TLPTs". We would welcome clarification that this refers only to DORA TLPTs and not to the financial institution's group-wide internal

red team policy. Internal teams carry out other testing activities that fall outside the remit of DORA and these activities should not be included in a defined policy. (does this not only apply if the institution chooses the option to perform TLPTs with internal testers - then red team)?

The option of commissioning internal testers is generally welcomed. The different treatment of internal and external testers is incomprehensible. Why should internally acquired qualifications depend on the length of service? What is the purpose of establishing a guideline for the assignment of internal testers that should not already be fulfilled by the selection of testers, the definition of the scope and an established risk management? We suggest: Internal testers, just like external testers, must have appropriate prior experience on relevant projects.

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

No

Cooperation between TLPT authorities: The RTS does not explain the scope of a TLPT if multiple TLPT authorities are involved. Extending the scope based on the views of multiple TLPT authorities would prolong any TLPT and increase the complexity of an audit.

Proposed amendment:

Article 12 (1): ''(c) consult the financial institution on whether other TLPT authorities could be involved or whether their activities in other Member States involve common ICT systems, internal teams and/or the same intragroup ICT service provider. The financial institution should provide evidence to the TLPT authority if cooperation could be useful."

Mutual recognition: We support the proposed mutual recognition of TLPTs in the Member States. However, Article 12 (5) seems to support mutual recognition only if it concerns "critical or important functions ... internal auditors ... and if the TLPT was conducted as a pooled test." An important criterion should be added: Has the TLPT tested the common ICT systems used by the financial institution in several Member States? Art. 12 (5) should be extended accordingly.

The report mentioned in Art. 26 (6) (Annex VII) "Details of the TLPT's summary test report" should contain information for mutual recognition of the test. In this report, a FE may provide further details on whether common ICT systems have been tested that are equally used by the financial institution in other Member States.

Article 12 (5): "... scope of testing, including the use of common ICT systems and relevant internal teams, whether or not they are internal ..."

Annex VII: ''(p) relevant information in relation to the mutual recognition of this test in other Member States where the financial institution operates"

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

Yes

Article 4.2a: It is correct that access to information on the TLPT should be on a need-to-know basis. However, the list of groups that have access to parts of the information should be extended. Several processes for organizing and financing a TLPT require members of the financial institution who are not

part of the control team or the governing body. An example in most tests is the procurement process, which requires some exceptions to this requirement. We recommend that the requirement be amended to allow for individual exceptions under the supervision of the test managers (or TLPT authority).

General Introduction (page 21) Section (18): The examples of possible exceptions should be clearly marked as examples, as not every control team can give testers access to every ICT system.

If a bank's systems are tested that are also used by other banks, these should be taken into account when designing or conducting the test.