JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

JC 2023 72

27 November 2023

Consultation Paper

Draft Regulatory Technical Standards specifying elements related to threat led penetration tests

JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

Contents

1. Responding to this consultation

The three European Supervisory Authorities (ESAs) invite comments on all matters in this paper and on the specific questions summarised in Annex II. Comments are most helpful if they:

– respond to the question stated;
– indicate the specific question to which the comment relates;
– contain a clear rationale and
– describe any alternatives ESAs should consider.

Submission of responses

The ESAs will consider all comments received by **04 March 2024.**

All contributions should be submitted online at www.esma.europa.eu under the heading 'Your input - Consultations'. Please note that comments submitted after this deadline or submitted via other means may not be processed.

Publication of responses

All contributions received will be published following the close of the consultation, unless you request otherwise. Please clearly and prominently indicate in your submission any part you do not wish to be publicly disclosed. A standard confidentiality statement in an email message will not be treated as a request for non-disclosure. A confidential response may be requested from us in accordance with the ESAs' rules on 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 ESAs' Boards of Appeal and the European Ombudsman.

Data protection

Information on data protection can be found at www.esma.europa.eu under the heading 'Data protection'.

2. Executive Summary

Reasons for publication

1. Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (hereinafter 'DORA') under its Article 26(11), tasks the ESAs, '*in agreement with the ECB*' to develop draft regulatory technical standards ('RTS') '*in accordance with the TIBER-EU framework*' to specify further the criteria used for identifying financial entities required to perform threat-led penetration testing, the requirements and standards governing the use of internal testers, the requirements in relation to scope, testing methodology and approach for each phase of the testing, results, closure and remediation stages and the type of supervisory and other relevant cooperation needed for the implementation of TLPT and for the facilitation of mutual recognition.

2. The ESAs have prepared this Consultation Paper (CP) to consult interested parties for the purpose of elaborating its draft RTS to be submitted to the European Commission (EC). Respondents to this consultation are encouraged to provide the relevant background information, and qualitative and quantitative data on costs and benefits, as well as concrete redrafting proposals, to support their arguments where alternative ways forward are called for. If respondents envisage any technical difficulties in implementing the proposed requirements, they are encouraged to provide details regarding the specific technical and operational challenges and specify the costs involved, which are important for the cost-benefit analysis.

Contents

3. Section 3 of this CP presents the background to our proposal and questions for your consideration and Section 4 includes our proposed draft RTS. Annex I includes a preliminary impact assessment and Annex II lists all questions formulated in this CP.

Next steps

4. The ESAs will consider the feedback received to this consultation in Q2 2024 and should publish a Final Report and the submission of the draft RTS to the European Commission by 17 July 2024.

5. The ESAs will finalise the impact assessment regarding the proposed measures, to be included in the Final Report to be submitted to the EC. Due to the limitation of the information available,

a more in-depth cost-benefit analysis will be provided after input of stakeholders. The input from stakeholders will help the ESAs in finalising the RTS and the relevant impact assessment. Therefore, respondents to this consultation are strongly encouraged to provide solutions for any problems raised and to support the drafting proposals with relevant data.

3. Background and rationale

3.1 Introduction

6. DORA sets out uniform requirements for the security of network and information systems of companies and organisations operating in the financial sector as well as critical third parties which provide ICT (Information Communication Technologies) services to them, such as cloud computing services, software solutions or data analytics services. DORA creates a regulatory framework on digital operational resilience, whereby all financial entities under this regulation need to make sure they can withstand, respond to, and recover from ICT-related disruptions and threats. These requirements are homogenous across the EU and across all financial subsectors.

7. In this context, the ESAs, through the Joint Committee, and in agreement with the ECB, have been empowered under Article 26(11) of DORA to deliver a draft RTS on certain aspects of advanced testing of ICT tools, systems and processes based on TLPT, in accordance with the TIBER-EU framework.

Mandate - Article 26(11) of DORA

The ESAs shall, in agreement with the ECB, develop joint draft regulatory technical standards in accordance with the TIBER-EU framework in order to specify further:

1. the criteria used for the purpose of the application of paragraph 8, second subparagraph[1];

2. the requirements and standards governing the use of internal testers;

3. the requirements in relation to:
(i) the scope of TLPT referred to in paragraph 2;
(ii) the testing methodology and approach to be followed for each specific phase of the testing process;
(iii) the results, closure and remediation stages of the testing;

4. the type of supervisory and other relevant cooperation which are needed for the implementation of TLPT, and for the facilitation of mutual recognition of that testing, in the context of financial entities that operate in more than one Member State, to allow an

[1] We consider that the mandate refers to Article 26(8), third subparagraph ("Competent authorities shall identify financial entities that are required to perform TLPT taking into account the criteria set out in Article 4(2), based on an assessment of the following: (a) impact–related factors, in particular the extent to which the services provided and activities undertaken by the financial entity impact the financial sector; (b) possible financial stability concerns, including the systemic character of the financial entity at Union or national level, as applicable; (c) specific ICT risk profile, level of ICT maturity of the financial entity or technology features involved.") rather than the second. A corrigendum of Article 26(11), first subparagraph, point (a) is expected to be published soon in that respect.

appropriate level of supervisory involvement and a flexible implementation to cater for specificities of financial sub-sectors or local financial markets.

When developing those draft regulatory technical standards, the ESAs shall give due consideration to any specific feature arising from the distinct nature of activities across different financial services sectors.

3.2 Drafting principles: DORA and the TIBER-EU framework

3.2.1 The TIBER-EU framework

8. TIBER-EU is a European framework for threat intelligence-based ethical red-teaming. It provides comprehensive guidance on how authorities, entities, threat intelligence and red-team providers should work together to test, maximise learning and improve the cyber resilience of entities by carrying out controlled cyberattacks. Inspired by and taking account of the lessons learned from similar initiatives in the United Kingdom (CBEST) and the Netherlands (TIBER-NL), it was developed jointly by the ECB and the EU's national central banks and published in May 2018.

9. For the implementation of the TIBER-EU framework, certain governance structures and processes must be adopted at the level of a jurisdiction by the authority(ies) in charge. The framework includes four areas and two types of requirements: those that are identified as "mandatory" in the framework, and a number of optional requirements (that can be adapted to the specificities of individual jurisdictions). The adoption of the TIBER-EU framework is voluntary but once adopted any implementation of TIBER-EU must adhere to the requirements deemed 'mandatory' for the purposes of the framework and the various implementations are reviewed at regular intervals to ensure harmonisation. So far Belgium, Denmark, Finland, Germany, Iceland, Ireland, Italy, Luxembourg, the Netherlands, Norway, Portugal, Romania, Spain, and Sweden have adopted and implemented it, whereas at least four other jurisdictions are working on an implementation.

3.2.2 Approach followed for developing the draft RTS 'in accordance with the TIBER-EU framework'

10. Once a jurisdiction decides to adopt the TIBER-EU framework, it shall implement the requirements, which are deemed mandatory for the adoption to be considered compliant with the TIBER-EU framework. However, the mandate established under Article 26(11) of DORA does not fully cover all requirements of the TIBER-EU framework. The aim of the provisions on TLPT included in Article 26 and 27 of DORA is to design an advanced digital operational resilience testing standard applicable to financial entities that are mature enough from an ICT perspective.

11. In most cases, jurisdictions that have implemented the TIBER-EU framework have chosen to do so on a voluntary basis for the entities in scope of the implementation (in limited cases, there have been mandatory implementations of the TIBER-EU framework enforced by the respective authority). Under DORA, once the TLPT requirements will apply, it will be compulsory across the EU for the financial entities in scope to undergo TLPTs at a frequency chosen by the TLPT authority or the competent authority according to the Member State implementation of articles 26.9 and 26.10 of DORA authority (every three years in general).

12. It should be noted that, for financial entities identified to be required to perform TLPT according to this Regulation, although only the DORA TLPT requirements are legally binding and as such prevail over the TIBER-EU framework, they have been drafted to be, within the mandate given in L1, in accordance with the TIBER-EU framework. Therefore, any jurisdiction who wishes to continue to use its own implementation of the TIBER-EU framework should be able to do so, incorporating any potential additional DORA TLPT requirements should they exist. The TIBER-EU framework and supplementary guidance as well as the various TIBER-EU implementations should thus be seen as providing additional guidance to the DORA TLPT requirements and not as replacing those legal requirements laid down in the RTS.

13. As to the drafting process of the RTS, an important element of the DORA Article 26(11) mandate is the fact that the draft technical standards should be developed "in accordance with the TIBER-EU framework". In this respect, the European Commission (EC) has clarified that:
    - there should be no dynamic reference to TIBER-EU in the RTS, and the RTS should transpose into requirements the relevant provisions of TIBER-EU i.e. which correspond to the mandate given in Article 26(11) of DORA and to standard RTS requirements.
    - the RTS should mirror as much as possible the TIBER-EU framework to ensure that it is 'in accordance' with TIBER-EU framework within the limits of the mandate of L1.

14. The RTS is therefore not meant to reproduce in full the detail of the TIBER-EU framework and all related guidance published by the ECB and under the various TIBER implementations as:
    - DORA mandate does not cover the entirety of the TIBER-EU framework;
    - On those aspects which are in scope of the mandate, the aim is to incorporate under DORA the requirements that are deemed 'mandatory' for the implementation of TIBER-EU with minor alterations where needed so that they can become legal requirements, to the extent possible.

3.2.3 Main differences between DORA TLPT and the TIBER-EU framework

15. **Authority conducting TLPT**. DORA allows Member States to designate a single public authority (SPA) who is then charged with all tasks and responsibilities related to TLPT in that Member State. It also allows for the delegation of only some of the tasks to another authority and it allows for the Competent Authority to retain all tasks and responsibilities related to TLPT. Hence, each Member State might select a different allocation of which tasks are carried out by which authority.

16. For the purposes of this RTS the concept of 'TLPT authority' has been created to cover the various cases. Such TLPT authority can therefore be any authority, which is responsible for the relevant TLPT-related task. Hence, it is possible to have multiple TLPT authorities per Member State.

17. **Case of pan-European competent authorities**. For credit institutions classified as significant in accordance with Article 6(4) of Regulation (EU) No 1024/2013, the ECB is tasked with all tasks and responsibilities related to TLPT for the said significant institutions. The ECB can however make use of Article 26(10) of DORA, which allows the delegation of some TLPT related tasks and responsibilities.

18. **Use of internal testers.** Although the use of internal testers is not foreseen in the TIBER-EU framework, DORA allows for it, "to take advantage of internal resources at corporate level", under certain conditions aiming at safeguarding the quality of the tests.

19. **Purple teaming exercise.** Purple teaming as a collaborative testing activity that involves both the red team testers and the blue team currently is a strongly encouraged but not yet mandatory element in the TIBER-EU framework. This Regulation makes purple teaming mandatory, similarly to the replay workshop.

20. The TIBER-EU framework should be updated to comply with these requirements.

3.3 Other general drafting principles

3.3.1 Cross-sectoral

21. The TLPT methodology and process set out in the proposed RTS does not include any sector-specific or entity-specific requirements (i.e. sector-agnostic and entity-agnostic requirements). This is in line with the sector agnostic approach taken by the TIBER-EU framework which has in the past been used for many different kinds of financial entities or even entities outside of the financial sector.

Q1. Do you agree with this cross-sectoral approach? If not, please provide detailed justifications and alternative wording as needed.

3.3.2 Proportionality

22. The proposed draft RTS includes the proportionality principle in the criteria that are used to identify financial entities required to perform TLPT. Only financial entities that carry a certain degree of systemic importance and are mature enough from an ICT perspective are required to perform a TLPT (as described in the following paragraphs).

23. Since all financial entities that are required to perform TLPT must meet a high level of ICT maturity and have to fulfil the further criteria set out in the proposed draft RTS, the testing methodology does not include any further proportionality considerations and measures.

Q2. Do you agree with this approach? If not, please provide detailed justifications and alternative wording as needed.

3.4 Approach on the identification of financial entities required to perform TLPT

24. For the identification of financial entities required to perform TLPT Article 26(8), third subparagraph of DORA states that these financial entities shall be identified taking into account the principle of proportionality according to Article 4(2) and based of the assessment of:
    (a) impact-related factors, in particular the extent to which disruption of the services provided and activities undertaken by the financial entity would impact the financial sector;
    (b) possible financial stability concerns, including the systemic character of the financial entity at Union or national level, as applicable;
    (c) specific ICT risk profile, level of ICT maturity of the financial entity or technology features involved.

25. Given the wide scope of DORA, and the above-mentioned criteria, the proposed RTS introduces a two-layered approach. For financial entities operating in core financial services subsectors and playing a systemic role, specific criteria and thresholds are given.

26. Additionally, in order to best reflect the mandate given to the ESAs ("*When developing those draft regulatory technical standards, the ESAs shall give due consideration to any specific feature arising from the distinct nature of activities across different financial services sectors*."[2]), criteria are specified in such a way to give the TLPT authority the possibility to opt-in further financial entities that fulfil the specified criteria. Moreover, specificities from different types of financial entities as well as the rationale given in recital 56 of DORA have been taken into account in the drafting of the specification of the criteria.

27. In order to reflect all aspects of the given mandate, the TLPT authority is given the possibility to opt-out financial entities from the requirement to perform TLPT that do not carry a certain degree of systemic importance and are not mature enough from an ICT perspective in order not to risk the continuity of core financial services.

28. Also the belonging to a group shall be considered in the identification of a financial entity by the TLPT authority if common ICT systems are used.

[2] Article 28(11), second subparagraph, of DORA

Q3. Do you agree with the two-layered approach proposed to identify financial entities required to perform TLPT? If not, please provide detailed justifications and alternative wording as needed.

Q4. 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? If not, please provide detailed justifications and alternative wording as needed.

3.5 Approach on the testing: scope, methodology, conclusion

29. The testing process prescribed by the RTS very closely follows the testing process outlined in the TIBER-EU Framework. The intention was to distil all requirements of the TIBER-EU testing process deemed 'mandatory' into a concise regulatory text.

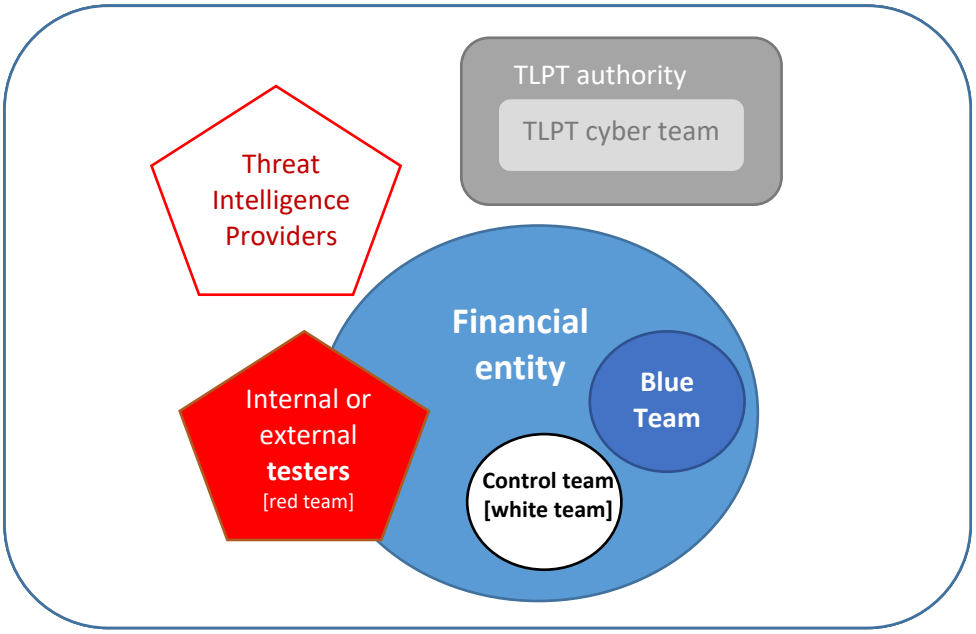
30. Nevertheless, some elements had to be altered owing to the different legal nature of a voluntary TIBER-EU Framework and a legally binding regulation. In general, the level of detail included in the TIBER-EU framework goes significantly beyond what can be replicated in an RTS.

31. As a concrete example, TIBER-EU prescribes at a very detailed level, which stakeholders have to meet for the various TIBER-EU workshops. While it was acknowledged that the TIBER-EU workshops hold a lot of value, they were nonetheless not included in the RTS as such. It was deemed preferable to leave some flexibility as to how the objective of each workshop is to be met. A recital nonetheless strongly encourages the parties involved in a TLPT to hold in-person or virtual meetings at various steps of the TLPT process, which are detailed.

Q5: Do you consider that the RTS should include additional aspects of the TIBER process? If so, please provide suggestions.

3.5.1 Testing methodology

32. **TLPT participants**. Similarly to the TIBER-EU framework, there are five types of participants in a TLPT, which are depicted in the Figure below:



33. The main stakeholders in a TLPT are:

- The **TLPT Cyber Team** (or TCT) mirrors the TIBER Cyber Team in the TIBER-EU framework. It is the staff within the TLPT authority where all operative TLPT-related matters are addressed. For example, it may be comprised of the test managers;
- The **control team** mirrors the white team under the TIBER-EU framework and manages the TLPT from the side of the financial entity undergoing the exercise. This includes all aspects from procurement of the external providers, the risk assessment the operational management of the day-to-day testing activities, risk management, etc. The control team lead should have the necessary mandate within the financial entity to guide all the aspects of the test, without compromising the secrecy of the test;
- The **blue team** is, similarly to the TIBER-EU framework, made up of those employees that are defending the financial entity against simulated or real cyber threat while not knowing that they are tested;
- The **threat intelligence provider**, similar to the TIBER-EU framework concept, mimics an hacker information gathering activity by using multiple reliable sources;
- DORA concept of '**testers'** is broader than that of 'red team' under the TIBER-EU framework as DORA permits the use of both internal and external testers. Tested entities may useboth types of testers as long as all requirements are complied with. Part of the ESA's mandate was to develop specific requirements applying to the use of internal testers (please see section 3.6 below).

34. **Risk management of the TLPT**. Carrying out TLPT is not without risk. Hence solid risk management throughout every stage of the TLPT is essential. The responsibility for the conduct of the test and the risk management thereof rests entirely with the financial entity undergoing TLPT. Financial entities must assess the risk of conducting TLPT prior to its commencement and continue to monitor this risk updating the risk assessment as needed.

Q6. Do you agree with the approach followed for financial entities to assess the risks stemming from the conduct of testing by means of TLPT? If not, please provide detailed justifications and alternative wording as needed.

35. A key way to minimize risk associated with TLPT is the selection of experienced, suitable and highly skilled testers and TI providers. As testing takes place on live production systems, only experienced providers should be selected.

36. Under TIBER-EU this selection of high-quality providers was ensured through the use of the TIBER-EU services procurement guidelines. Under TIBER-EU the entity being tested should carry out due diligence to make sure its chosen providers meet all the requirements set out in the TIBER-EU service procurement guidelines.

37. Under DORA requirements for testers are laid out in Article 27 DORA. However, due to the critical nature of TLPT and in order to ensure accordance with TIBER-EU, further criteria for testers and threat intelligence providers were included in this draft RTS. These requirements come from the TIBER-EU services procurement guidelines but have been adapted for the purpose of being included in a regulatory technical standard.

Q7. Do you consider the proposed additional requirements for external testers and threat intelligence providers are appropriate? If not, please provide detailed justifications and alternative wording or thresholds as needed.

Q8. 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? If not, please provide detailed justifications and alternative wording as needed.

3.5.2 Testing process

38. The process established in the proposed RTS very closely follows the TIBER-EU testing process sequence of phases, as follows:

39. The preparation phase closely resembles the TIBER-EU preparation phase. In this phase the control team is formed, the scoping takes place,the threat intelligence providers and the testers are selected and as the case may be, procured.

40. The testing phase also closely resembles the process described in the TIBER-EU framework. It is broken down into a threat intelligence part, which ultimately produces the scenarios, which are to be tested during the red teaming part of the testing phase. The active red teaming test has to be a minimum of 12 weeks.

41. The closing phase also resembles the process described in the TIBER-EU framework. During the closure phase, the TLPT is revealed to the blue team and the red team and blue team reports are drafted. Blue team and red team come together to replay relevant defensive and offensive actions carried out during the test, a purple teaming exercise will take place and ultimately a test summary report and remediation plan will be prepared by the financial entity and shared with the TLPT authority.

42. Finally, the TLPT authority will issue an attestation that the TLPT was carried out in accordance with this regulation, identifying which critical systems were in scope of the TLPT.

Q9. Do you consider the proposed process is appropriate? If not, please provide detailed justifications and alternative wording as needed.

43. **Pooled testing**. Under DORA[3] 'pooled testing' designates a case where several financial entities will participate in a TLPT, for which ICT third-party services provider will directly procure an external tester, but only if it is reasonably expected that the non-pooled test have an adverse impact on:
    a. the quality or security of services delivered by the ICT third-party service provider to customers that are entities falling outside the scope of DORA, or
    b. the confidentiality of the data related to such services.

44. Specific requirements relating to pooled testing have been introduced regarding the remediation plan (Article 11), the cooperation of TLPT authorities (Article 14(2)) and the attestation (Article 15(5)).

Q10. Do you consider the proposed requirements for pooled testing are appropriate? If not, please provide detailed justifications and alternative wording as needed.

3.6 Approach on the use of internal testers

45. Article 26(11) of DORA requires the ESAs to define "*requirements and standards governing the use of internal testers*".

[3] Article 26(4) of Regulation (EU) 2022/2554

46. The possibility introduced currently in DORA to use internal testers is justified "in order to take advantage of internal resources available at corporate level"[4]. However, given the very sensitive nature of TLPTs, some safeguards have been established, both on the testers themselves and on their use by the financial entity.

47. As already mentioned, this is an important divergence from the current TIBER-EU framework, which so far only allows to use testers that are external to the tested entity. However, the possibility to use internal testers, is expected to be added in future revision of the TIBER-EU framework.

48. The starting point for the drafting of this part of the RTS was that these testers should carry out TLPTs as effectively and safely as external testers, without the security or the activity of the financial entity being endangered.

49. In that respect, as to the qualities to be displayed by the internal testers themselves, DORA already establishes the same general requirements for all testers alike, both internal and external. They are requirements[5] of highest suitability and reputability, necessary technical and operational capabilities and expertise, certification, provision of independent assurance of sound risk management of risks associated with the carrying out of TLPT and coverage by professional indemnity insurances. As described in section 3.5.1 detailed requirements for external testers are introduced as a safeguard for the financial stability as tests are performed on live production systems.

50. As to the use of internal testers by financial entities, DORA already establishes two types of safeguards: the first one is the obligation to use external testers every three tests[6]. As a second set of safeguards, the following requirements apply the use of internal testers[7]: prior supervisory approval, the absence of conflict of interest within the financial entity and the mandatory use of an external threat intelligence provider.

51. Considering the abovementioned existing requirements regarding the use of internal testers, and on the need to secure as much as possible the activities of testers in a TLPT, the ESAs' proposal requires financial entities to establish certain specific arrangements to ensure that TLPTs conducted by internal testers will not have detrimental impacts on financial entities using them on the financial entity itself, by putting too much pressure on its resources and on the conduct of the TLPT itself.

52. The proposed additional requirements for the financial entity are:

(a) Define a policy for the management of internal testers in TLPTs;

[4] Recital 61 of Regulation (EU) 2022/2554

[5] Article 27(1) of DORA

[6] Article 26(8), first subparagraph of DORA provides that "When financial entities use internal testers for the purpose of undertaking TLPT, they shall contract external testers every three tests."

[7] Article 27(2) of DORA

(b) Establish measures to ensure that the use of internal testers will not negatively impact the financial entity's capability regarding ICT-related incidents, or the availability of resources devoted to ICT-related tasks during the carrying out of a TLPT;

(c) Establish measures to ensure internal testers have sufficient resources and capabilities to conduct a TLPT.

53. The draft RTS clarifies that an internal testing team should consist of a test lead and two members and provides limitations with respect to the period of employment of the testing team members for the financial entity. These measures shall ensure that all internal testing team members are indeed internal staff in order to take advantage of the knowledge accumulated by such internal testers on the tested financial entity. Furthermore, it is important to have training requirements to ensure internal testers can deploy up-to-date skills.

54. The proposal also contains a requirement to mention the use of internal testers in all documents to be produced for the purpose of the TLPT (e.g. the Red Team Test Plan or the attestation).

55. The ESAs' proposal also clarifies who should be considered as an "internal tester". Specifically, a tester who is not directly employed by the financial entity but by an ICT intra-group service provider[8] of the financial entity shall also be considered as an internal tester.

Q11. Do you agree with the proposed requirements on the use of internal testers? If not, please provide detailed justifications and alternative wording as needed.

3.7 Approach on cooperation

56. Article 26(11) of DORA requires the ESAs to specify "*the type of supervisory and other relevant cooperation which are needed for the implementation of TLPT, and for the facilitation of mutual recognition of that testing, in the context of financial entities that operate in more than one Member State, to allow an appropriate level of supervisory involvement and a flexible implementation to cater for specificities of financial sub-sectors or local financial markets*."

57. At this stage, the ESAs consider that while cooperation between the authorities of a single Member State should be left to that Member States to organise, the draft RTS should cover cases where cooperation is needed between authorities from different Member States.

58. Under DORA, tests will be organised at the level of a financial entity by the TLPT authority of its home Member State.

[8] Defined as an undertaking providing ICT services in Article 3(20) of DORA.

59. The first case for cooperation between the TLPT authority of the home Member State of a financial entity and other authorities is for financial entities providing services in other Member states through freedom of provision of services or through the establishment of a branch in other Member States where one or more critical or important functions are fully or partially operated by the financial entity. From a legal point of view, a subsidiary is a financial entity according to Article 2 of DORA.

60. In such case, the TLPT authority of the home Member State will have to identify, contact and ask the TLPT authorities in such host Member States if they want to be involved in the planned TLPT and to which extent they want to be involved. The level of involvement is ranging from receiving information to participating in the TCT established by the TLPT authority of the home Member state of the financial entity.

61. **Groups**. Another case for cooperation between TLPT authorities is when TLPT authorities decide to organise joint TLPTs on several financial entities established in different Member States but belonging to the same group.

62. In such case, the TLPT authorities of the financial entities performing the test shall agree among themselves as to which one of them should lead the TLPT.

Q12. Do you consider the proposed requirements on supervisory cooperation are appropriate? If not, please provide detailed comments and alternative wording as needed.

Q13. Do you have any other comment or suggestion to make in relation to the proposed draft RTS? If so, please provide detailed justifications and alternative wording as needed.

4. Draft Regulatory Technical Standards

COMMISSION DELEGATED REGULATION (EU) …/…

of XXX

supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying the criteria used for identifying financial entities required to perform threat-led penetration testing, the requirements and standards governing the use of internal testers, the requirements in relation to scope, testing methodology and approach for each phase of the testing, results, closure and remediation stages and the type of supervisory and other relevant cooperation needed for the implementation of TLPT and for the facilitation of mutual recognition.

(Text with EEA relevance)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011[9], and in particular Article 26(11), fourth subparagraph thereof,

Whereas:

(1) This Regulation has been drafted in accordance with the TIBER-EU framework and mirrors the methodology, process and structure of TLPT as described in TIBER-EU. Financial entities subject to TLPT may refer to and apply the TIBER-EU framework as long as that framework is consistent with the requirements set out in Articles 26 and 27 of Regulation (EU) 2022/2554 and this Regulation.

(2) The designation of a single public authority responsible for TLPT-related matters at national level according to Article 26(9) of Regulation (EU) 2022/2554 shall be without prejudice to the competence for the TLPT of competent authorities entrusted with supervision at Union level of certain financial entities to which Regulation (EU) 2022/2554 applies, such as, for instance, the European Central Bank for significant credit institutions. Where only some tasks are delegated in a Member

9 OJ L 333, 27.12.2022, p. 1.

State in accordance with the national implementation of Article 26(10) of Regulation (EU) 2022/2554, the competent authority in accordance with Article 46 of Regulation (EU) 2022/2554 remains TLPT authority for those tasks not delegated.

(3) Authorities responsible for TLPT matters should ensure that financial entities operating in core financial services subsectors (including credit institution, payment and electronic money institutions, central security depositories, central counterparties, trading venues, insurance and reinsurance undertakings) perform TLPT where relevant criteria indicating their systemic impact are met. However, authorities responsible for TLPT matters should exclude from TLPT those financial entities for which, even though they meet the sector-specific criteria identified in this Regulation, in light of an overall assessment of their of ICT maturity, impact and financial stability impact, the TLPT is not justified.

(4) In the assessment of the criteria to identify financial entities required to perform TLPT, TLPT authorities should carefully consider whether the ICT maturity of the financial entity is sufficient to undergo advanced testing in the form of TLPT, and exclude entities from performing TLPT where their ICT maturity is not sufficient to carry out tests on live production systems.

(5) Financial entities may be part of a financial group. Where such group includes other financial entities and uses common ICT systems, authorities responsible for TLPT matters should consider the group structure and systemic character at national or Union level in the assessment of whether a financial entity should be subject to TLPT.

(6) Similarly to the TIBER-EU framework, the testing methodology developed in this Regulation requires the involvement of the following main participants: the financial entity, with a control team (mirroring the TIBER-EU so-called 'white team') and a blue team, the TLPT authority, in the form of a TLPT cyber team (mirroring the TIBER-EU so-called 'TIBER cyber teams'), a threat intelligence provider and testers (mirroring the TIBER so-called 'red team provider'). In order to ensure that the TLPT benefits from the experience developed in the framework of TIBER-EU implementation and to reduce the risks associated to the performance of TLPT, this Regulation ensures that the responsibilities of the TLPT cyber teams to be set up at the level of TLPT authorities match as closely as possible those of the TIBER cyber teams under TIBER-EU. These TLPT cyber teams should, normally, include test managers responsible for overseeing the TLPT. These test managers should have sufficient skills and capabilities to provide advice and challenge tester proposals. Building on the experience under the TIBER-EU framework, it has proven to be valuable to have a team of at least two test managers assigned to each test. To reflect that the TLPT is used to encourage the learning experience, and unless they have capacity or cability issues, TLPT authorities are strongly

encouraged to consider that for the duration of a TLPT, test managers should not conduct supervisory activities on the same financial entity undergoing a TLPT.

(7) The secrecy of a TLPT is of utmost importance to ensure that the conditions of the test are realistic, therefore, testing should be covert, and precautions should be taken in order to keep the TLPT confidential, including the choice of codenames designed in such a way as not allowing the identification of the TLPT by third parties. Should staff members responsible for the security of the financial team be aware of a planned or ongoing TLPT, it is likely that they would be more observant and alert than during normal working conditions, thereby resulting in an altered outcome of the test. Therefore, staff members of the financial entity outside of the control team should be made aware of any planned or ongoing TLPT only in presence of cogent reasons and subject to prior agreement of the test managers. This may for example be to ensure the secrecy of the test in case a blue team member has detected the test.

(8) As evidenced through the experience gathered in the TIBER-EU framework with respect to the 'white team', the selection of an adequate control team lead (CTL) is indispensable for the safe conduct of a TLPT. The CTL should have the necessary mandate within the financial entity to guide all the aspects of the test, without compromising the confidentiality of the test. Aspects such as deep knowledge of the financial entity, the CTL's job role and strategic positioning, seniority and access to the management board should be considered for the purposes of the appointment. The control team should be as small as possible in order to reduce the risk of compromising the TLPT.

(9) There are inherent elements of risks associated with TLPT as critical functions are tested in live production environment, with the possibility of causing denial-of-service incidents, unexpected system crashes, damages to critical live production systems, or the loss, modification, or disclosure of data, highlights the need for robust risk management measures. Hence, it is very important that financial entities are at all points aware of the particular risks that arise in a TLPT and that these are mitigated, to ensure the TLPT is conducted in a controlled manner all along the test. In that respect, it is essential that the testers and threat intelligence providers have the highest level of skills and expertise and an appropriate experience in threat intelligence and TLPT in the financial services industry to be able to deliver effective and most qualified professional services.

(10) Intelligence-led red team tests differ from conventional penetration tests, which provide a detailed and useful assessment of technical and configuration vulnerabilities often of a single system or environment in isolation, but contrary to the former, do not assess the full scenario of a targeted attack against an entire entity, including the complete scope of its people, processes and technologies. During the selection process, financial entities should ensure that testers possess the requisite skills to perform intelligence-led red team tests, and not only penetration tests.

(11) In order to apply the testing process specified in this Regulation to pooled testing, specific requirements have been introduced to specify that the designated financial entity referred to in Article 26(4) of Regulation (EU) 2022/2554 is in charge of providing all necessary documentation and monitoring the test process laid down in this Regulation, towards the lead TLPT authority referred to in Article 12(2) of this Regulation, but the obligations of each financial entity participating in the pooled testing remain unaffected during the pooled test.

(12) As evidenced by the experience of the implementations of the TIBER-EU framework, holding in-person or virtual meetings including all relevant stakeholders (financial entity, authorities, testers and threat intelligence providers) is the most efficient way to ensure the appropriate conduct of the test. Therefore in-person and virtual meetings are strongly encouraged and should be held at various steps of the process, and in particular: during the preparation phase at the launch of the TLPT and to finalise on its scope; during the testing phase, to finalise the threat intelligence report and the red team test plan and for the weekly updates; and during the closure phase, for the purposes of replaying testers and blue team actions, purple teaming and to exchange feedback on the TLPT.

(13) In order to ensure the smooth performance of the TLPT, the authority competent for the TLPT (TLPT authority) should clearly present its expectations with respect to the test to the financial entity. In that respect, the team internal to the TLPT authority should ensure that an appropriate flow of information is established with the control team within the financial entity, with the testers and threat intelligence providers if they have been selected. If the testers and TI provider are not involved during the scoping process, they should receive detailed information on the agreed scoping, to facilitate a smooth transition to the next phase of threat intelligence gathering.

(14) The threat intelligence provider should collect intelligence or information that cover at least two key areas of interest, the targets, by identifying potential attack surfaces across the financial entity and the threats, by identifying relevant threat actors and probable threat scenarios in order to provide the testers with the information needed to simulate a real-life and realistic attack on the financial entity's live systems underpinning its critical or important functions. In order to ensure that the threat intelligence provider considers the relevant threats for the financial entity, the threat intelligence provider should exchange on the draft threat intelligence report and on the draft red team test plan with the testers, the control team and the test managers. The threat intelligence provider may take into account a generic threat landscape provided by the TLPT authority for the financial sector of a member state, if applicable, as a baseline for the national threat landscape.

(15) It is essential that, prior to the red team test phase of the TLPT, the testers receive detailed explanations on the threat intelligence report and analysis of possible threat

scenarios from the threat intelligence provider, to allow the tester to gain insight and further review the scope specification document and target treat intelligence report to finalise the red team test plan.

(16) It is important that sufficient time be allocated to the active red team testing phase to allow testers to conduct a realistic and comprehensive test in which all attack phases are executed, and flags are reached. The time allocated should be determined taking into account the TLPT scope, the entity's resources, any external requirements for a given TLPT and the availability of supporting information supplied by the financial entity.

(17) During the active red team testing phase, the testers should deploy a range of tactics, techniques and procedures (TTPs) to adequately test the live production systems of the financial entity. The TTPs should include, as appropriate, reconnaissance (i.e. collecting as much information as possible on a target), weaponization (i.e. analysing information on the infrastructure, facilities and employees and preparing for the operations specific to the target), delivery (i.e. the active launch of the full operation on the target), exploitation (i.e. where the testers' goal is to compromise the servers, networks of the financial entity and exploit its staff through social engineering), control and movement (i.e. attempts to move from the compromise systems to further vulnerable or high value ones) and actions on target (i.e. gaining further access to compromise systems and acquiring access to the previously agreed target information and data, as previously agreed in the red team test plan).

(18) While carrying out a TLPT, testers should act considering the time available to perform the attack, resources and ethical and legal boundaries. Should the testers be unable to progress to the programmed next stage of the attack, occasional assistance should be provided by the control team, upon agreement of the TLPT authority, in the form of 'leg-ups', where the financial entity gives access, as appropriate, to ICT system or internal network to continue with the test and focus on the following attack steps.

(19) It is necessary that the TLPT is used as a learning experience to enhance the digital operational resilience of financial entities. In that respect, the blue team and testers should replay the attack and review the steps taken in order to learn from the testing experience in collaboration with the testers. Additionally, a purple teaming exercise should be carried out to maximize the learning experience. Methods such as table-top exercises, catch-and-release exercises, collaboratively developing a "proof-of-concept" for selected TTPs or techniques such as war gaming may be used for the purple teaming.

(20) To further facilitate the learning experience of all parties involved in the TLPT, for the benefit of future tests and to further the digital operational resilience of

financial entities parties concerned should provide feedback to each other on the overall process, and in particular identifying which activities progressed well or could have been improved, which aspects of the TLPT process worked well or could be improved.

(21) Competent authorities referred to in Article 46 of Regulation (EU) 2022/2554 and TLPT authorities, where different, should work together to incorporate advanced testing by means of TLPT into the existing supervisory processes. In that respect it is appropriate that, especially, for the test summary report and remediation plans, a close cooperation between test managers who were involved in the TLPT and the responsible supervisors is established, in order to share the correct understanding of the TLPT findings and of how they should be interpreted.

(22) Financial entities should ensure that, as required by Article 26(8), first subparagraph, of Regulation (EU) 2022/2554, every three tests they contract external testers. Where financial entities include in the team of testers both internal and external testers, this should be considered as a TLPT performed with internal testers for the purposes of Article 26(8), first subparagraph, of Regulation (EU) 2022/2554.

(23) This Regulation is based on the draft regulatory technical standards submitted to the Commission by the European Banking Authority, the European Insurance and Occupational Pensions Authority, the European Securities and Markets Authority (European Supervisory Authorities), in agreement with the European Central Bank.

(24) The Joint Committee of the European Supervisory Authorities has conducted open public consultations on the draft regulatory technical standards on which this Regulation is based, analysed the potential related costs and benefits and requested the advice of the Banking Stakeholder Group established in accordance with Article 37 of Regulation (EU) No 1093/2010 of the European Parliament and of the Council[10], the Insurance and Reinsurance Stakeholder Group and the Occupational Pensions Stakeholder Group established in accordance with Article 37 of Regulation (EU) No 1094/2010 of the European Parliament and of the Council[11] and the Securities and Markets Stakeholder Group established in accordance with Article 37 of Regulation (EU) No 1095/2010 of the European Parliament and of the Council[12],

[10] Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/78/EC (OJ L 331, 15.12.2010, p. 12).

[11] Regulation (EU) No 1094/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Insurance and Occupational Pensions Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/79/EC (OJ L 331, 15.12.2010, p. 48).

[12] Regulation (EU) No 1095/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Securities and Markets Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/77/EC (OJ L 331, 15.12.2010, p. 84).

HAS ADOPTED THIS REGULATION:

CHAPTER I

GENERAL PROVISIONS

Article 1

Definitions

For the purposes of this Regulation, the following definitions shall apply:

(1) ‘control team’ means the team composed of staff of the tested financial entity and staff of its third-party service providers, as needed, who knows about, and manages the test.

(2) ‘control team lead’ means the staff member of the financial entity responsible for the conduct of all TLPT-related activities for the financial entity in the context of a given test;

(3) ‘blue team’ means the staff of the financial entity and of the financial entity’s third-party service providers, that are defending a financial entity's use of network and information systems by maintaining its security posture against simulated or real attacks and that is not aware of the TLPT;

(4) ‘purple teaming’ means a collaborative testing activity that involves both the red team testers and the blue team;

(5) ‘TLPT authority’ means:

a. the single public authority that is designated to be responsible for carrying out TLPT in a Member State in accordance with Article 26(9) of Regulation (EU) 2022/2554, or

b. the authority to which the exercise of some or all of the tasks in relation to TLPT is delegated in accordance with Article 26(10) of Regulation (EU) 2022/2554, or

c. the competent authority in accordance with Article 46 of Regulation (EU) 2022/2554;

(6) ‘TLPT Cyber Team’ or ‘TCT’ means the staff within the TLPT authority(ies), that is responsible for TLPT-related matters;

(7) 'test managers' means staff designated to lead the activities of the TLPT authority for a specific TLPT to monitor compliance with the requirements of this Regulation;

(8) 'threat intelligence provider' means the expert(s), external to the financial entity, who collect and analyse targeted threat intelligence relevant for the financial entities in scope of a specific TLPT exercise and develop matching relevant and realistic threat scenarios;

(9) 'leg-up' means the assistance or information provided by the control team to the testers to allow the testers to continue the execution of an attack path where they are not able to advance on their own, including for insufficient time or resources in a given TLPT;

(10) 'attack path' means the route followed by testers during the active red team testing phase of the TLPT in order to reach the flags defined for that TLPT;

(11) 'flags' are key objectives in the ICT systems supporting critical or important functions of a financial entity that the testers try to achieve through the test;

(12) 'sensitive information' means information that can readily be leveraged to carry out attacks against the ICT systems of the financial entity, intellectual property, confidential business data and/or personal data that can directly or indirectly harm the company and its ecosystem would it fall in the hands of malicious actors;

(13) 'pool' means all the financial entities participating in a pooled TLPT pursuant to Article 26(4) of Regulation (EU) 2022/2554;

(14) 'home Member State' means the Member State in which a financial entity is established as defined in applicable sectoral legislation;

(15) 'host Member State' means host Member State in accordance with applicable sectoral legislation;

CHAPTER II

CRITERIA TO IDENTIFY FINANCIAL ENTITIES REQUIRED TO PERFORM TLPT

Article 2

Identification of financial entities required to perform TLPT

1. TLPT authorities shall require all of the following financial entities to perform TLPT:

(a) Credit institutions identified as global systemically important institutions (G-SIIs) in accordance with Article 131 of Directive 2013/36/EU of the European Parliament and of the Council [13] or as other systemically important institutions (O-SIIs) or that are part of a G-SIIs or O-SIIs.

(b) Payment institutions, exceeding in each of the previous two financial years EUR 120 billion of total value of payment transactions as defined in point (5) of Article 4 of Directive (EU) 2015/2366 of the European Parliament and of the Council[14].

(c) Electronic money institutions, exceeding in each of the previous two financial years EUR 120 billion of total value of payment transactions as defined in point (5) of Article 4 of Directive (EU) 2015/2366 or EUR 40 billion of total value of the amount of outstanding electronic money.

(d) Central securities depositories;

(e) Central counterparties;

(f) Trading venues with an electronic trading system that meet at least one of the following criteria:

(i) at national level, the trading venue which has the highest market share in terms of turnover in equity, or in equity-like, financial instruments or in bonds and other forms of securitised debts, or in derivative contracts or in other non-equity financial instruments in each of the preceding two financial years;

(ii) at Union level, the trading venue whose Union market share in terms of turnover in equity, or in equity-like, financial instruments or in bonds and other forms of securitised debts or in derivative contracts or in other non-equity financial instruments exceeds 5% in each of the preceding two financial years; where the trading venue is part of a group,

[13] Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC (OJ L 176, 27.6.2013, p. 338).

[14] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (OJ L 337, 23.12.2015, p. 35).

the turnover of financial instruments on all trading venues pertaining to the same group and established in the Union shall be considered.

(g) Insurance and reinsurance undertakings that meet the following criteria in a subsequent manner, identifying:

(i) first, the undertakings exceeding in each of the previous two financial years EUR 500 million of Gross Written Premium (GWP).

(ii) secondly, undertakings that fulfil point (i) included in the 90th percentile of the Gross Written Premiums (GWP) distribution including all undertaking having reported Gross Written Premiums above the average of the Gross Written Premiums of all insurance and reinsurance undertaking established in the Member State calculated separately for the following activities:

- Life other than life Similar-To-Health (SLT) and reinsurance life,

- Non-Life other than non-life Similar-To-Health (NSLT) and reinsurance non-life.

- Health calculated as the sum of life Similar-To-Health (SLT) and non-life Similar-To-Health (NSLT) and

- Reinsurance calculated as the sum of reinsurance life and reinsurance non-life.

(ii) Third, insurance and reinsurance undertakings that fulfil point (ii) and whose total assets is equal or higher to the 10 % of the sum of the total assets valuated according to Article 75 of Directive 2009/138/EC of the insurance and reinsurance undertakings established in the Member State belonging to the activity type identified as referred to in point (ii);

2. Financial entities referred to in points (a) to (g) of paragraph 1 shall not be required to carry out TLPT where the assessment of the criteria listed in paragraph 3 indicates that the impact of the financial entity, financial stability concerns relating to it or its ICT risk profile do not justify the performance of the test. Where more than one financial entity belonging to the same group and using common ICT systems or the same ICT intra-group service provider meet the criteria set out in points (a) to (g) of paragraph 1, the TLPT authority(ies) of the Member State(s) where these financial entities are established may, in consultation with the TLPT authority of the Member State where the parent undertaking of such group is established, decide if the requirement to perform TLPT on an individual basis is relevant for these financial entities.

3. TLPT authorities shall assess whether any financial entities other than those referred to in paragraph 1 shall be required to perform TLPT, on the basis of all of the following criteria:

(a) impact-related and systemic character related factors:

a. the size of the financial entity, determined taking into account whether the financial entity provides financial services in the national or Union market and by comparing

the activities of the financial entity to those of other financial entities providing similar services. Where possible, the TLPT authority shall consider the market share position at national and EU level, the range of activities offered by the financial entity and the market share of the services provided or of the activities undertaken at national and at Union level;

b. the extent and nature of the interconnectedness of the financial entity with other financial entities in the financial sector at national and Union level;

c. the criticality or importance of the services provided to the financial sector;

d. the substitutability of the services provided by the financial entity;

e. the complexity of the business model of the financial entity and the related services and processes. Where possible, the TLPT authority shall consider whether the financial entity operates more than one business models and the interconnectedness of different business processes and the related services;

f. whether the financial entity is part of a group of systemic character at Union or national level in the financial sector and using common ICT systems;

(b) ICT risk related factors:

a. the risk profile of the financial entity;

b. the threat landscape of the financial entity;

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

d. the complexity of the ICT architecture of the financial entity;

e. 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;

f. outcomes of any supervisory reviews relevant for the assessment of the ICT maturity of the financial entity;

g. the maturity of ICT business continuity plans and ICT response and recovery plans;

h. the maturity of the operational ICT security detection and mitigation measures including the ability to monitor the financial entity's ICT infrastructure on a permanent basis, to detect ICT-related events in real time, to analyse events, to respond to them in a timely and effective manner;

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

CHAPTER III

REQUIREMENTS REGARDING TEST SCOPE, TESTING METHODOLOGY AND RESULTS OF TLPT

Section I

TESTING METHODOLOGY

Article 3

TCT and TLPT Test Managers

1. A TLPT authority shall assign the responsibility for coordinating TLPT-related activities to a TCT. A TCT shall include test managers that are assigned to oversee an individual TLPT.
2. For each test there shall be a test manager and at least one alternate.
3. The test managers shall monitor and ensure that the requirements laid out in this Regulation are complied with.

Article 4

Organisational arrangements for financial entities

1. Financial entities shall appoint a control team lead who is responsible for the day-to-day management of the test and the decisions and actions of the control team.
2. Financial entities shall establish organisational and procedural measures ensuring that:
   a. access to information pertaining to any planned or ongoing TLPT is limited on a need-to-know basis to the control team, the management body, the testers, the threat intelligence provider and the TLPT authority;
   b. the control team consults the test managers prior to involving any member of the blue team in a TLPT;
   c. 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;
   d. arrangements relating to the secrecy of the TLPT, applicable to staff of the financial entity, to the staff of relevant ICT third party service providers, to testers and to the threat intelligence provider are in place.
   e. The control team shall provide any information pertaining to the TLPT to the TCT upon request.

f. Where possible, parties involved in the TLPT shall refer to it by code name only.

Article 5

Risk management for TLPT

1. During the preparation phase referred to in Article 7, the control team shall conduct an assessment of the risks associated with the testing of live production systems of critical or important functions of the financial entity, including potential impacts on the financial sector, as well as on financial stability at Union or national level, and shall review it throughout the conduct of the test.

2. The control team shall take measures to manage the risks referred to in paragraph 1 and in particular shall ensure that:
   a. the threat intelligence provider and external testers provide copies of certifications that are appropriate according to recognised market standards for the performance of their activities;
   b. the threat intelligence provider and external tester are duly and fully covered by relevant professional indemnity insurances, including against risks of misconduct and negligence;
   c. the threat intelligence provider provide at least three references from previous assignments related to intelligence-led red team tests;
   d. the external testers provide at least five references from previous assignments related to intelligence-led red team tests;
   e. the staff of the threat intelligence provider assigned to the TLPT shall:
      i. be composed of at least a manager with at least five years of experience in threat intelligence, including three years of collecting, analysing and producing threat intelligence for the financial sector as well as at least one additional member with at least two years of experience in threat intelligence;
      ii. display a broad range and appropriate level of professional knowledge and skills including intelligence gathering tactics, techniques and procedures, geopolitical, technical and sectorial knowledge as well as adequate communication skills to clearly present and report on the result of the engagement.
      iii. have a combined participation in at least three previous assignments related to threat intelligence-led red team tests;
   f. for external testers, the staff of the red team assigned to the TLPT shall:
      i. be composed of at least the a manager, with at least five years of experience in threat intelligence-led red team testing as well as at least

two additional testers, each with red teaming experience of at least two years;

ii. display a broad range and appropriate level of professional knowledge and skills, including, knowledge about the business of the financial entity, reconnaissance, risk management, exploit development, physical penetration, social engineering, vulnerability analysis, as well as adequate communication skills to clearly present and report on the result of the engagement;

iii. have a combined participation in at least five previous assignments related to threat intelligence-led red team tests;

g. external testers and threat intelligence providers carry out restoration procedures at the end of testing, including secure deletion of information related to passwords, credentials and other secret keys compromised during the TLPT, secure communication to the financial entities of the account compromised, secure collection, storage, management, and disposal of data collected;

h. in addition to the restoration procedures at the end of testing as referred to in point (e), external testers shall carry out the following restoration procedures:

i. command and control deactivation;

ii. scope and date kill switch(es);

iii. removal of backdoors and other malware;

iv. potential breach notification;

v. procedures for future back-up restauration which may contain malware or tools installed during the test;

vi. monitoring the blue team activities and informing the control team of any possible detections; and

i. external testers and the threat intelligence provider are prohibited from the following activities:

i. unauthorised destruction of equipment of the financial entity and of its ICT third-party service providers, if any;

ii. uncontrolled modification of information and ICT assets of the financial entity and of its ICT third-party service providers, if any;

iii. intentionally compromising the continuity of critical or important functions of the financial entity;

iv. unauthorised inclusion of out-of-scope systems;

v. unauthorised disclosure of test results.

The control team shall keep record of the documentation provided by the external testers and the threat intelligence providers to demonstrate compliance with the points (a) to (g) above, including detailed curriculum vitae of the staff of the external tester and of the threat intelligence provider employed for the TLPT.

3. In its risk assessment and management, the control team shall at minimum consider the following types of risks related to:

   a. selecting and entering into the contractual arrangement with the threat intelligence provider and external testers, where applicable, and the confidentiality of the information they gain access to;

   b. lack of compliance of the TLPT with Regulation (EU) 2022/2554 and with this Regulation resulting in lack of the attestation referred to in Article 26(7) of Regulation (EU) 2022/2554, including where due to breaches of confidentiality on the TLPT or to lack of ethical conduct;

   c. crisis and incident escalation;

   d. active red team phase, including risks related to interruption of critical activities and corruption of data through activities of the testers;

   e. blue team activity, including risks related to interruption of critical activities and corruption of data through activities of the blue team;

   f. incomplete restauration of systems affected by the TLPT.

Section II

Testing Process

Article 6

Preparation phase

1. The financial entity shall submit the initiation documents to the TLPT authority within three months from having received a notification from the TLPT authority that a TLPT shall be carried out. The initiation documents shall consist of all of the following:

   a. a project charter including a high-level project plan, containing the information set out in Annex I;

   b. the contact details of the control team lead;

   c. information on intended use of internal or external testers or both, where relevant as detailed in Article 13;

   d. information on the communication channels to be used during the TLPT;

   e. the code name for the TLPT.

2. The TLPT authority shall assess and validate the initiation documents of the financial entity.

3. Following the validation of the initiation documents by the TLPT authority, the financial entity shall set up a control team that shall support the control team lead in its tasks of:

   a. defining communications channels and processes within the control team, with the testers and the threat intelligence providers in all matters related to the TLPT;

   b. informing the management body of the financial entity about the progress of the TLPT and the associated risks;

   c. taking decisions based on subject matter expertise throughout the TLPT;

   d. executing the TLPT in compliance with the requirements set out in this Regulation;

   e. selecting the threat intelligence provider for the TLPT;

   f. selecting the external testers, the internal testers or both; and

   g. preparing the scope specification document.

4. The scope specification document shall contain all information set out in Annex II and be submitted to the TLPT authority within six months from the receipt of the notification from the TLPT authority referred to in paragraph 1. The scope specification document shall be approved by the management body of the financial entity.

5. Financial entities shall consider the following criteria for the inclusion of critical or important functions in the scope of the TLPT:

   a. the criticality or importance of the function and its possible impact to the financial sector and on financial stability at national and Union level;

   b. the importance of the function for the day-to-day business operations of the financial entity;

   c. the exchangeability of the function;

   d. the interconnectedness with other functions;

   e. the geographical location of the function;

   f. the sectoral dependence of other entities on the function;

   g. the symbolic or political status of the function;

   h. where available, threat intelligence concerning the function.

6. The control team shall share the initiation documents and the scope specification document with the testers and threat intelligence providers once these are contracted.

The control team shall inform the testers and threat intelligence providers about the testing process to be followed.

7. Prior to the testing phase, the control team shall consult the TLPT authority on the TLPT risk assessment and on the risk management measures that the control team intends to take. The TLPT authority may object to the risk assessment and to the related risk management measures should they not adequately address the risks of the TLPT.

8. The control team shall assess the compliance of threat intelligence providers and external testers they consider involving in the TLPT with the requirements laid out in Article 27 of Regulation (EU) 2022/2554 and with Article 5(2) of this Regulation. The control team shall select provider(s) in accordance with its risk and document the outcome of the assessment of the TLPT and risk management practices. Prior to contracting the selected threat intelligence provider and external tester, the control team shall provide evidence of such compliance to the TLPT authority. The TLPT authority may object to the selected threat intelligence providers and external testers where they do not ensure compliance with Article 5(2) or national security legislations.

9. The TLPT authority shall inform the financial entity of their approval of the scope specification document.

Article 7

Testing phase: Threat intelligence

1. Following approval of the scope specification document by the TLPT authority, the threat intelligence provider shall analyse generic and sector-specific threat intelligence relevant for the financial entity. The threat intelligence provider shall identify cyber threats and discovered or potential vulnerabilities concerning the financial entity. Furthermore, the threat intelligence provider shall gather information on, and analyse concrete, actionable and contextualized target and threat intelligence concerning the financial entity, including through consulting the control team and the test managers.

2. The threat intelligence provider shall present the relevant threats and targeted threat intelligence, and propose appropriate scenarios to the control team, testers and test managers. The proposed scenarios shall differ with reference to the identified threat actors and associated tactics, techniques and procedures and shall target each and every critical or important functions in the scope of the TLPT.

3. The control team shall select at least three scenarios to conduct the TLPT, on the basis of all of the following elements:

(a) the recommendation by the threat intelligence provider and the threat-led nature of each scenario;

(b) the input provided by the test managers;

(c) the feasibility of the proposed scenarios for execution, based on the expert judgement of the testers;

(d) the size, complexity and overall risk profile of the financial entity and the nature, scale and complexity of its services, activities and operations.

4. At maximum one of the selected scenarios may be non-threat-led and be based on a forward looking and potentially fictive threat with high predictive, anticipative, opportunistic or prospective value given the anticipated developments of the threat landscape faced by the financial entity.

5. The threat intelligence provider shall provide the targeted threat intelligence report to the control team, including the scenarios selected according to paragraphs 2, 3 and 4. The threat intelligence report shall include the information set out in Annex III.

6. The control team shall submit the targeted threat intelligence report to the TLPT authority for approval. The TLPT authority shall inform the financial entity of their approval.

Article 8

Testing phase: Red Team Test

1. Following approval of the threat intelligence report by the TLPT authority, the testers shall prepare the red team test plan that shall include the information set out in Annex IV. The testers shall use the scope specification document and the targeted threat intelligence report as a basis for producing the attack scenarios.

2. The testers shall consult the control team, the threat intelligence provider and the test managers on the red team test plan, including the communication, procedural and project management arrangement, the preparation and use-cases for leg-up activation, and the reporting agreements to the control team and test managers.

3. The red team test plan shall be approved by the control team and TLPT authority. The TLPT authority shall inform the financial entity of their approval.

4. Upon approval of the red team test plan in accordance with paragraph 3, the testers shall carry out the TLPT during the active red team testing phase.

5. The duration of the active red team testing phase shall be proportionate to the scope and complexity of the financial entity, and in any case shall at least be twelve weeks. The control team, the threat intelligence provider, the testers and the TLPT authority shall agree on the end of the active red team testing phase.

6. Any changes to the red team test plan subsequent to its approval, including to the timeline, scope, target systems or flags, shall be approved by the control team and the TLPT authority.

7. During the entire active red team testing phase, testers shall report at least weekly to the control team and test managers on the progress made in the TLPT, and the threat intelligence provider shall remain available for consultation and additional threat intelligence when requested by the control team.

8. The control team shall timely provide leg-ups designed on the basis of the red team test plan. Leg-ups may be added or adapted upon approval by the control team and the TLPT authority.

9. In case of detection of the testing activities by any staff member of the financial entity or of its ICT third-party service providers, where relevant, the control team, in consultation with the testers and without prejudice to paragraph 10, shall propose and submit measures allowing to continue the TLPT to the TLPT authority for validation while ensuring its secrecy.

10. Under exceptional circumstances triggering risks of impact on data, damage to assets, and disruption to critical or important functions, services or operations at the financial entity itself, its counterparts or to the financial sector, the control team lead may suspend the TLPT, or if the continuation of the TLPT is not otherwise possible and subject to prior validation by the TLPT authority, continue the TLPT using a limited purple teaming exercise.

11. At any time during the active red team testing phase, the control team, the testers, the blue team, the threat intelligence provider and the test managers may agree on whether to repeat specific parts of the TLPT and/or on carrying out purple teaming exercise.

Article 9

Closure phase

1. Following the end of the active red team testing phase, the control team shall inform the blue team that a TLPT took place.

2. Within four weeks from the end of the active red team testing phase, the testers shall submit to the control team a red team test report containing the information set out in Annex V.

3. Without undue delay, the control team shall provide the red team test report to the blue team and test managers. Upon request by the test managers, a version of the red team test report that does not contain any sensitive information shall be submitted to the test managers.

4. Upon receipt of the red team test report, and no later than four weeks after, the blue team shall submit to the control team a blue team test report containing the information set out in Annex VI. Without undue delay, the control team shall provide the blue team test report to the testers and the test managers. Upon request by the test managers, a version of the blue team test report that does not contain any sensitive information shall be submitted.

5. Within four weeks from the sharing of the blue team test report referred to in paragraph 4, the blue team and the testers shall carry out replay of the offensive and defensive actions performed during the test. The control team shall in addition conduct a purple teaming exercise on topics jointly identified by the blue team and the testers, based on vulnerabilities identified during the test and, where relevant, on issues that could not be tested during the active red team testing phase.

6. After completion of the replay and purple teaming exercises, the control team, the blue team, the testers and threat intelligence providers shall provide feedback to each other on the TLPT process. The test manager may provide feedback.

7. The control team shall prepare a report summarizing the relevant findings of the TLPT referred to in Article 26(6) of Regulation (EU) 2022/2554, which shall not contain any sensitive information, containing the information set out in Annex VII. Within 12 weeks from the completion of the active red team testing phase, the control team shall submit the test summary report to the TLPT authority for approval.

Article 10

Remediation plan

(1) Within 16 weeks from the ending of the active red team testing phase, the financial entity shall provide the remediation plans referred to in Article 26(6) of Regulation (EU) 2022/2554 to the TLPT authority and, where different, to the financial entity's competent authority.

(2) The remediation plan referred in paragraph 1 shall include, for each finding occurred in the framework of the TLPT:

a. a description of the identified shortcomings;

b. a description of the proposed remediation measures and of their prioritisation and expected completion, including where relevant measure to improve the identification, protection, detection and response capabilities;

c. a root cause analysis;

d. the financial entity's staff or functions responsible for the implementation of the proposed remediation measures or improvements;

e. the risks associated to not implementing the measures referred to in point (b) and, where relevant, risks associated to the implementation of such measures.

(3) In case of pooled testing each financial entity participating in the pooled TLPT shall provide a remediation plan according to paragraph 1.

CHAPTER IV

REQUIREMENTS AND STANDARDS GOVERNING THE USE OF INTERNAL TESTERS

Article 11

Use of internal testers

1. Financial entities shall establish all of the following arrangements for the use of internal testers:

   (a) the definition and implementation of a policy for the management of internal testers in a TLPT. Such policy shall:

      i. include criteria to assess suitability, competence, potential conflicts of interest of the testers and define management responsibilities in the testing process. The policy shall be documented and periodically reviewed;

      ii. provide that the internal testing team includes a test lead, and at least two additional members. The policy shall require that all members of the test team have been employed by the financial entity or by an ICT intra-group service provider for the preceding two years;

      iii. include provisions on training on how to perform red teaming of the internal testers.

   (b) measures to ensure that the use of internal testers to perform TLPT will not negatively impact the financial entity's general defensive or resilience capabilities regarding ICT-related incidents or significantly impact the availability of resources devoted to ICT-related tasks during a TLPT;

   (c) measures to ensure that internal testers have sufficient resources and capabilities available to perform TLPT in accordance with this Regulation;

(d) when a TLPT authority approves the use of internal testers according to Article 27(2)(a) of Regulation(EU) 2022/2554, the TLPT authority shall consider the requirements laid down in Article 5(2) of this Regulation.

2. When using internal testers, the financial entity shall ensure that such use is mentioned in the following documents:

   (a) the test initiation documents referred to in Article 6;

   (b) the red team test report referred to in Article 9(2);

   (c) the report summarizing the relevant findings of the TLPT referred to in Article 26(6) of Regulation (EU) 2022/2554.

3. For the purposes of this Regulation, testers employed by an ICT intra-group service provider shall be considered as internal testers of the financial entity.

CHAPTER V

COOPERATION AND MUTUAL RECOGNITION AND FINAL PROVISIONS

Article 12

Cooperation

1. For the purposes of conducting a TLPT in relation to a financial entity operating in more than one Member State, the TLPT authority of the home Member State shall:

   a. determine which TLPT authorities in host Member States may be involved, taking into account whether one or more critical or important functions are operated in, or shared across, host Member States;

   b. inform the TLPT authorities identified according to point (a) of the decision to carry out a TLPT test on the financial entity. Within 20 working days from the receipt of the information on a future conduct of a TLPT, the TLPT authorities of the host Member States may either express their interest in following the TLPT as observers or assign a test manager to participate in the TCT established by the TLPT authority designated as lead in accordance with paragraph 2.

   Unless otherwise agreed by the TLPT authorities of the home Member State and of the host Member States, the TLPT authority of the home Member State shall lead the TLPT.

   The lead TLPT authority shall provide all TLPT authorities acting as observers in TLPT with the scope specification document, the test summary report, remediation plan and attestation. The lead TLPT authority shall coordinate all participating TLPT authorities throughout the TLPT and adopt all the decisions necessary to carry out the TLPT.

The lead TLPT authority may set a maximum number of participating TLPT authorities, where the efficient conduct of the TLPT might otherwise be compromised.

2. For the purposes of conducting pooled testing as referred to in Article 26(4) of Regulation (EU) 2022/2554, the TLPT authority of the designated financial entity shall lead the TLPT unless otherwise agreed by the TLPT authorities of the other financial entities participating in the pooled test.

3. For the purposes of conducting a joint TLPT in relation to more than one financial entity belonging to the same group and using common ICT systems or the same ICT intra-group service provider, the TLPT authorities of the financial entities performing such joint TLPT shall agree on which TLPT authority shall lead the TLPT.

4. Where, in relation to a financial entity required to perform a TLPT, its TLPT authority differs from its competent authority as referred to in Article 46 of Regulation (EU) 2022/2554, these authorities shall share any relevant information in respect of all TLPT-related matters for the purposes of carrying out the TLPT or to carry out their duties in accordance with Regulation (EU) 2022/2554.

5. For the purposes of mutual recognition of a TLPT, the attestation referred to in Article 26(6) of Regulation (EU) 2022/2554 shall indicate the scope of the TLPT, including the reference to the critical or important functions in the scope of test, whether internal testers were used and if the TLPT was performed as a pooled test. Where relevant, the attestation shall include information on functions in the scope of the TLPT in relation to which the TLPT was not performed. Where relevant to facilitate the mutual recognition, TLPT authorities shall share relevant information relating to the TLPT carried out.

6. Where several TLPT authorities have been involved in a TLPT, the attestation shall be provided by the lead TLPT authority.

Article 13

Entry into force and application

This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels,

For the Commission

The President

ANNEX I

Content of the project charter

Item of information	Information required
Person responsible for the project plan, i.e. the Control Team Lead	Name Contact details
Testers	☐ internal ☐ external ☐ both
Communication channels selected in accordance with Article 7, including: (a) Email encryption to be used (b) Online data rooms to be used (c) Instant messaging to be used	
Codename for the TLPT	
If any, critical or important functions the financial entity operates in other Member States	1. List of critical or important functions operated in another Member State 2. for each critical or important function, indication of the Member State or States in which they are operated
If any, critical or important functions supported by ICT third party service providers	3. List of critical or important functions supported by ICT third-party service providers 4. for each function, identification of the ICT third party service provider
Expected deadlines for the completion of the:	
(1) Preparation Phase, in accordance with Article 6	yyyy-mm-dd

(2) Testing Phase, in accordance with Articles 7 and 8:	yyyy-mm-dd
(3) Closure Phase, in accordance with Article 9	yyyy-mm-dd
(4) Remediation plan in accordance with Article 10	yyyy-mm-dd

ANNEX II

Content of the scope specification document

1. The scope specification document shall include a list of all critical or important functions identified by the financial entity.

2. For each identified critical or important function, the following information shall be included:

(a) Where the critical or important function is not included in the scope of the TLPT, the explanation of the reasons for which it is not included;

(b) Where the critical or important function is included in the scope of the TLPT:

(i) the explanation of the reasons for its inclusion;

(ii) the identified ICT system(s) supporting this critical or important function;

(iii) for each identified ICT system:

1. whether it is outsourced and if so, the name of the ICT third party service provider;
2. the jurisdictions in which the ICT system is used;
3. a high-level description of preliminary flag(s), indicating which security aspect of confidentiality, integrity, authenticity and/or availability is covered by each flag.

ANNEX III

Content of the targeted threat intelligence report

The threat intelligence report shall include information on all of the following:

1. Overall scope of the intelligence research including at least the following:
    a. critical functions in scope;
    b. their geographical location;
    c. official EU language in use;
    d. relevant ICT third party services providers;
    e. period of time over which the research is gathered.
2. Overall assessment of what concrete actionable intelligence can be found about the financial entity, such as:
    a. Employee usernames and passwords found on the internet;
    b. Look-alike domains which can be mistaken for official domains of the financial entity;
    c. Technical reconnaissance: vulnerable and/or exploitable software, systems and technologies;
    d. information posted by employees on social media, related to the financial entity, which might be used for the purposes of an attack;
    e. Information for sale on the dark web;
    f. Any other relevant information available on the internet or public networks;
    g. Where relevant, physical targeting information, including ways of access to the premises of the financial entity.
3. Threat intelligence analysis considering the general threat landscape and the particular situation of the financial entity, including, at least:
    a. Geopolitical environment;
    b. Economic environment;
    c. Technological trends and any other trends related to the activities in the financial services sector;

4. Threat profiles of the malicious actors (specific individual/group or generic class) that may target the financial entity, including the systems of the financial entity that malicious actors are most likely to compromise or target, the possible motivation, intent and rationale for the potential targeting and the possible modus operandi of the attackers.

5. Threat scenarios: At least three end-to-end threat scenarios for the threat profiles identified in accordance with point 4 who exhibit the highest threat severity scores. The threat scenarios shall describe the end-to-end attack path and shall include, at least:

   a. one scenario that includes but is not limited to compromised service availability;

   b. one scenario that includes but is not limited to compromised data integrity;

   c. one scenario that includes but is not limited to compromised information confidentiality.

6. Where relevant, description of the scenario referred to in Article 7(5).

ANNEX IV

Content of the red team test plan

The red team test plan shall include information on all of the following:

(i) communication channels and procedures;

(ii) the tactics, techniques and procedures allowed and not-allowed for use in the attack including ethical boundaries for social engineering, and how the privacy of involved parties is being safeguarded;

(iii) risk management measures to be followed by the testers;

(iv) a description for each scenario, including:

a. the simulated threat actor;

b. their intent, motivation and goals;

c. the target function(s) and the supporting ICT system or systems;

d. the targeted confidentiality, integrity, availability and authenticity aspects;

e. flags;

(v) a detailed description of each expected attack path, including pre-requisites and possible leg-ups to be provided by the control team, including deadlines for their provision and potential usage;

(vi) scheduling of red teaming activities, including time planning for the execution of each scenario, at a minimum split according to the three phases a tester takes throughout the testing phase, respectively entering financial entities' ICT systems, moving through the ICT systems and ultimately executing actions on objectives and eventually extracting itself from the ICT systems (in, through and out phases);

(vii) particularities of the financial entities' infrastructure to be considered during testing;

(viii) if any, additional information or other resources necessary to the testers for executing the scenarios.

ANNEX V

Content of the red team test report

The red team test report shall include information on at least all of the following:

(a) Information on the performed attack, including:

a. the targeted critical or important functions and identified ICT systems, processes and technologies supporting the critical or important function, as identified in the red team test plan;

b. summary of each scenario;

c. flags reached and not reached;

d. attack paths followed successfully and unsuccessfully;

e. tactics, techniques and procedures used successfully and unsuccessfully;

f. deviations from the red team test plan, if any;

g. leg-ups granted, if any;

(b) all actions that the testers are aware of that were performed by the blue team and the period of time needed by the blue team to:

a. reconstruct all details of the attack;

b. identify remaining artefacts, such as scripts or programs, left behind in the systems by the testers;

c. collect all relevant logs;

d. collect all relevant indicators of compromise (IOCs);

(c) discovered vulnerabilities and other findings, including:

a. vulnerability and other finding description including their criticality;

b. root cause analysis of successful attacks;

c. recommendations for remediation including indication of the remediation priority.

ANNEX VI

Content for the blue team test report as referred to in Article 13(4)

The blue team test report shall include information on at least of the following:

1. for each attack step described by the testers in the red team test report:

(a) list of detected attack actions;

(b) log entries corresponding to these detections;

2. assessment of the findings and recommendations of the testers;

3. evidence of the attack by the testers collected by the blue team;

4. blue team root cause analysis of successful attacks by the testers;

5. list of lessons learned and identified potential for improvement;

6. list of topics to be addressed in purple teaming.

ANNEX VII

Details of the test summary report of the TLPT

The test summary report shall include information on at least of the following:

(a) the parties involved;

(b) the project plan;

(c) the validated scope, including the rationale behind the inclusion or exclusion of critical or important functions and identified ICT systems, processes and technologies supporting the critical or important functions covered by the TLPT;

(d) selected scenarios and any significant deviation from the threat intelligence;

(e) executed attack paths, and used tactics, techniques and procedures;

(f) captured and non-captured flags;

(g) deviations from the red team test plan, if any;

(h) blue team detections, if any;

(i) purple teaming in testing phase, where conducted and the related conditions;

(j) leg-ups used, if any;

(k) risk management measures taken;

(l) identified vulnerabilities and other findings, including their criticality;

(m) root cause analysis of successful attacks;

(n) high level plan for remediation, linking the vulnerabilities and other findings, their root causes and remediation priority;

(o) lessons derived from feedback received.

5. Annex I: Draft impact assessment

(1) As per Article 15(1) of Regulation (EU) No 1093/2010 (EBA Regulation), of Regulation (EU) No1094/2010 (EIOPA Regulation) and Regulation (EU) No 1095/2010 (ESMA regulation), any draft regulatory technical standards developed by the ESAs shall be accompanied by an Impact Assessment (IA) which analyses 'the potential related costs and benefits'.

(2) This analysis presents the IA of the main policy options included in this Consultation Paper (CP) on regulatory technical standards (RTS) to specify on certain aspects of advanced testing of ICT tools, systems and processes based on TLPT, in accordance with the TIBER-EU framework.

Problem identification

(3) Complexity of information and communication technology (ICT) risk is increasing and frequency of ICT-related incidents, including cyber incidents, is rising together with their potential significant adverse impact on the financial institutions' operational functioning. Moreover, due to the interconnectedness between financial institutions, ICT related incidents risk causing potential systemic impact.

(4) DORA introduces the requirement for advanced testing of ICT tools, systems and processes based on TLPT, in accordance with the TIBER-EU framework for financial entities that carry a certain degree of systemic importance and are mature enough from an ICT perspective.

(5) In this context, the ESAs, through the Joint Committee, and in agreement with the ECB, have been empowered under Article 26(11) of DORA to deliver a draft RTS to specify further the criteria used for identifying financial entities required to perform threat-led penetration testing, the requirements and standards governing the use of internal testers, the requirements in relation to scope, testing methodology and approach for each phase of the testing, results, closure and remediation stages and the type of supervisory and other relevant cooperation needed for the implementation of TLPT and for the facilitation of mutual recognition.

Policy objectives

(6) The draft RTS aims at specifying certain aspects of advanced testing of ICT tools, systems and processes based on TLPT, in accordance with the TIBER-EU framework aims to establish common requirements for the criteria used for identifying financial

entities required to perform threat-led penetration testing, the requirements and standards governing the use of internal testers, the requirements in relation to scope, testing methodology and approach for each phase of the testing, results, closure and remediation stages and the type of supervisory and other relevant cooperation needed for the implementation of TLPT and for the facilitation of mutual recognition.

Baseline scenario

(7) With the entry into force of DORA, financial entities that are identified according to Article 26(8) DORA are required to perform advanced testing of ICT tools, systems and processes based on TLPT and must comply with the requirements set out in Article 26 and 27 DORA as well as the additional requirements set out in this draft RTS.

(8) The above legal requirements form the baseline scenario of the impact assessment, i.e. the impact caused by DORA is not assessed within this impact assessment, which focuses only on areas where further specifications have been provided in the draft RTS

(9) The following overarching aspects have been considered when developing the proposed RTS.

POLICY ISSUE 1: IDENTIFICATION AND GROUP STRUCTURES

Options considered

(10) Financial entities can be organised in groups according to Article 2(11) of Directive 2013/24/EU. In these groups several financial entities might use the same common ICT systems for example by a common intra-group ICT service provider.

(11) As the identification criteria of Article 26(8) of DORA have to be applied on the level of financial entity only. The circumstance that a financial entity or several financial entities are part of a group that uses same common ICT systems might not be considered in the assessment to identify financial entities required to perform TLPT. Where several financial entities of the same group fulfil the criteria in Article 2 and are using the same common ICT systems, each identified financial entity of that group might be required to perform a TLPT on its own (option A).

(12) Another option could be where several financial entities are part of a group using the same common ICT systems or the same ICT service third-party provider, the TLPT authority or authorities as applicable consider the group structure in the assessment

for the identification of financial entities to be required to perform a TLPT and can select specific financial entities of that group (option B).

Cost-benefit analysis

(13) If several financial entities of a group that uses the same common ICT systems are required to perform a TLPT on its own, the same ICT systems are tested through TLPTs. Accordingly to the reasoning of the frequency of three years to repeat a TLPT, this re-testing of the same common ICT systems brings less further benefits compared to the higher efforts. If the financial entities in the group are of highest importance, this could be regulated by changing the testing frequency accordingly.

(14) By considering the fact that a financial entity may be part of a group with commonly used ICT systems, the same ICT systems can be tested in a regular manner and the resources can be better used.

Preferred option

(15) Option B is preferred.

POLICY ISSUE 2: APPROACH FOR THE IDENTIFICATION

Options considered

(16) DORA has a wide scope including several different types of financial entities as listed in its Article 2(1). Moreover, Article 26(8) states that financial entities shall be identified taking into account the principle of proportionality according to Article 4(2) and based of the assessment of:

a. impact-related factors, in particular the extent to which disruption of the services provided and activities undertaken by the financial entity would impact the financial sector;

b. possible financial stability concerns, including the systemic character of the financial entity at Union or national level, as applicable;

c. specific ICT risk profile, level of ICT maturity of the financial entity or technology features involved.

(17) Simple qualitative criteria that take three given dimensions into account and cover all types of financial entities that are in the scope of DORA reflecting any specific feature arising from the distinct nature of activities across different financial services sectors do not exist.

(18) In order to reflect the given criteria in Article 26(8) and any specific feature arising from the distinct nature of activities across different financial services sectors for the various types of financial entities, the given criteria could be specified for each single type of financial entities (option A).

(19) Another option is to specify qualitative criteria for specific types of financial entities that are of most relevance according to the criteria in Article 26(8) in order to have some common level of harmonisation across the Union and to give the competent authorities the possibility to opt-in or opt-out financial entities based on specific feature arising from the distinct nature of activities across different financial services sectors within the given criteria (option B).

Cost-benefit analysis

(20) The specification of a comprehensive list of qualitative criteria is not future-proof. Absolute thresholds needs to be updated on a regular basis and the relevance of different business models might change over time. Moreover, different member states have different specific features which might also be taken into account.

Preferred option

(21) Option B is preferred.

POLICY ISSUE 3: PURPLE TEAMING

Options considered

(22) The TIBER-EU framework includes purple teaming only as an optional element which may or may not be made mandatory by national TIBER implementations.

(23) One possibility is to therefore not include purple teaming at all in RTS as only mandatory elements of the TIBER-EU framework must be included in the RTS for it to be considered to be “in accordance” with TIBER-EU. (Option A)

(24) However, given that TIBER-EU allows for purple teaming as a strongly encouraged but not yet mandatory element and given that some jurisdictions have made purple teaming mandatory in their national TIBER implementation, another option is to include purple teaming in the RTS. (Option B)

Cost-benefit analysis

(25) Experience at national TIBER implementations has shown that purple teaming generally generates a significant amount of learning for the institution involved. It allows for a much greater blue team engagement in the closure phase and facilitates knowledge transfer between red and blue team.

(26) The cost of carrying out the purple teaming exercise, on the other hand, are not that significant when seen in comparison with the learnings achieved and in relation to the overall cost of a TLPT.

Preferred option

(27) Option B is preferred

POLICY ISSUE 4: ADDITIONAL REQUIREMENTS ON TESTERS AND THREAT INTELLIGENCE PROVIDERS

Options considered

(28) DORA Article 27 includes requirements for testers and TI providers in which are qualitative in nature and are significantly less detailed than the requirements included in the TIBER-EU Procurement Guidelines.

(29) One option is to not formulate any additional requirements to what is included in DORA. (Option A)

(30) The alternative is to include the key requirements for testers and TI providers from the TIBER-EU Procurement Guidelines.

Cost-benefit analysis

(31) Carrying out a TLPT on live production systems is inherently risky and DORA requires the most significant financial entities in the European Union to undergo such TLPT. Should any of these financial entities suffer an incident during a TLPT, the ramifications may not remain limited to said financial entity.

(32) A key way of mitigating the risks involved in a TLPT is to select providers who are of the highest skill and who have a lot of experience, not just in penetration testing in general, but in TLPT in particular.

(33) Clear, concise and verifiable criteria, such as the ones included in the TIBER-EU procurement guidelines - simplify the selection process the financial entities undergoing TLPT have to perform. Without these additional criteria a greater burden would rest on the financial entities to perform their due diligence on the providers they wish to select.

(34) On the other hand, having criteria which are too restrictive is likely to significantly limit the market of available providers who can carry out the TLPT. Considering that TLPT and red teaming in general is a relatively young industry, an already small market is further reduced by further criteria.

(35) Criteria referring to the number of years of experience are further going to act as a barrier of entry for new providers, thus naturally limiting the expansion potential of the market.

(36) Further, providers with the most experience in TLPT tend to be from countries outside of the European Union. DORA TLPTs will reveal highly sensitive information about financial entities which are often considered to be part of the national critical infrastructure. Hence there may be some reservations about procuring these services from providers from outside of the Union.

(37) The TIBER-EU procurement guidelines mitigated some of these limitations by being only guidelines which did not have to be precisely adhered to. No such middle ground is available for this RTS.

Preferred option

(38) Option B is preferred. Despite the aforementioned downsides to including additional, hard requirements on testers and TI providers, the security of the financial entity undergoing TLPT must be of the utmost importance.

6. Annex II: Overview of the questions for consultation

Q1. Do you agree with this cross-sectoral approach? If not, please provide detailed justifications and alternative wording as needed.

Q2. Do you agree with this approach? If not, please provide detailed justifications and alternative wording as needed.

Q3. Do you agree with the two-layered approach proposed to identify financial entities required to perform TLPT? If not, please provide detailed justifications and alternative wording as needed.

Q4. 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? If not, please provide detailed justifications and alternative wording as needed.

Q5: Do you consider that the RTS should include additional aspects of the TIBER process? If so, please provide suggestions.

Q6. Do you agree with the approach followed for financial entities to assess the risks stemming from the conduct of testing by means of TLPT? If not, please provide detailed justifications and alternative wording as needed.

Q7. Do you consider the proposed additional requirements for external testers and threat intelligence providers are appropriate? If not, please provide detailed justifications and alternative wording or thresholds as needed.

Q8. Do you think that the specified number of years of experience for external testers and threat intelligence providers is an appropriate measure to ensure external testers and threat intelligence providers of highest suitability and reputability and the appropriate knowledge and skills? If not, please provide detailed justifications and alternative wording as needed.

Q9. Do you consider the proposed process is appropriate? If not, please provide detailed justifications and alternative wording as needed.

Q10. Do you consider the proposed requirements for pooled testing are appropriate? If not, please provide detailed justifications and alternative wording as needed.

Q11. Do you agree with the proposed requirements on the use of internal testers? If not, please provide detailed justifications and alternative wording as needed.

Q12. Do you consider the proposed requirements on supervisory cooperation are appropriate? If not, please provide detailed comments and alternative wording as needed.

Q13. Do you have any other comment or suggestion to make in relation to the proposed draft RTS? If so, please provide detailed justifications and alternative wording as needed.