JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

JC 2024 29

17 July 2024

Final Report

Draft Regulatory Technical Standards specifying elements related to threat led penetration tests under Article 26(11) of Regulation (EU) 2022/2554

JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

Contents

1. 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 (TLPT), 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. Section 2 of this report presents in detail the mandate and background to the final draft RTS which is included in Section 3.

2. This report follows a consultation paper (CP) which presented a first draft of the RTS and 32 questions and was open to comments from the public from 8 December 2023 to 4 March 2024.

3. A total of 111 responses were received to the public consultation, covering all sectors. The ESAs have also received input from the ESAs' Stakeholders Groups.

4. Respondents appeared to be very concerned with the requirements applying to TLPT providers (both testers and threat intelligence providers), which were mostly deemed too strict considering the limited availability of these providers on the existing market. The proposed testing process has also been massively commented, including many requests for more clarity, in particular in respect of TLPTs involving several financial entities and an ICT service provider (in case of pooled testing or joint test), and for more time in particular for the closure phase. The feedback received is presented in detail in Sections 5 and 6.

5. The ESAs assessed the concerns raised to decide which changes, if any, should be made to the draft RTS. In the light of the comments received, the ESAs agreed with some of the proposals and their underlying arguments and have introduced changes to the draft RTS.

6. The main changes relate to: (i) the criteria to be used to select insurance and reinsurance undertakings required to perform TLPT by default, which have been revised to allow for more predictability for market stakeholders (ii) TLPTs involving several financial entities and/or ICT service providers (intragroup or third parties) in pooled TLPTs and joint TLPTs, with clarifications of the related processes which also require extended cooperation between the

involved TLPT authorities, and (iii) the requirements applicable to testers, external and internal, and threat intelligence providers, which have been revised to include different criteria on past experience and more flexibility, in conjunction with appropriate risk management measures.

7. More information on the feedback received and how this was taken on board by the ESAs is provided in Section 2, and in more detail in Sections 5 and 6.

Next steps

8. The ESAs will submit the final draft RTS to the European Commission for adoption. Following its adoption in the form of a Commission Delegated Regulation, it will then be subject to scrutiny of the European Parliament and the Council before publication in the Official Journal of the European Union.

9. The expected date of application of these technical standards is 17 January 2025.

2. Background and rationale

2.1 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, 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.

2.2 Drafting principles: DORA and the TIBER-EU framework

2.2.1 The TIBER-EU framework

8. TIBER-EU is a European framework for threat intelligence-based ethical red-teaming. TIBER-EU tests mimic the tactics, techniques and procedures of real-life attackers, based on bespoke threat intelligence. They are tailor-made to simulate an attack on the critical functions of an entity and its underlying systems, i.e. its people, processes and technologies. The outcome is not a pass or fail; instead the test is intended to reveal the strengths and weaknesses of the tested entity, enabling it to reach a higher level of cyber maturity.

9. The TIBER-EU framework 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.

10. 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 Austria, Belgium, Denmark, Finland, France, Germany, Iceland, Ireland, Italy, Luxembourg, the Netherlands, Norway, Portugal, Romania, Spain, and Sweden have adopted and implemented it, whereas at least two other jurisdictions are working on an implementation.

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

11. 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.

12. 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).

13. It should be noted that, for financial entities required to perform TLPT, only the DORA TLPT requirements are legally binding and as such prevail over the TIBER-EU framework. However, 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.

14. 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.
    - 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.

15. 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.

2.2.3 Main differences between DORA TLPT and the original TIBER-EU framework

16. **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. Article 26(10) of DORA 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.

17. 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.

18. **Case of pan-European competent authorities**. It should be noted that for certain categories of financial entities, competent authorities are not national authorities but pan-European ones, such as ESMA for trade repositories, credit rating agencies or critical benchmark providers or the ECB for credit institutions classified as significant in accordance with Article 6(4) of Regulation (EU) No 1024/2013. In the latter case, the ECB is tasked with all TLPT-related matters for the said significant institutions, but can however make use of Article 26(10) of DORA, which allows the delegation of some TLPT related tasks and responsibilities.

19. **Use of internal testers.** Although the use of internal testers is not foreseen in the original 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.

20. **Purple teaming exercise.** Purple teaming is a collaborative testing activity that involves both the red team (the testers) and the blue team (the staff from the attacked financial entity – for more details on the participants to a TLPT, please see section 2.5.1 below). It is currently strongly encouraged but not a mandatory element in the original TIBER-EU framework. This Regulation makes purple teaming mandatory in the closure phase, similarly to the replay workshop.

21. The TIBER-EU framework will be updated to comply with these requirements.

2.3 Other general drafting principles

2.3.1 Cross-sectoral

22. 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. The vast majority of the comments received in the public consultation agreed with this cross-sectoral approach.

2.3.2 Proportionality

23. 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).

24. 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.

25. A number of respondents to the public consultation requested that proportionality be included also in the requirements relating to the performance of the test, i.e. lightening the requirements for smaller or less significant entities. This is actually already taken into account, as, according to Article 26 of DORA, TLPT is an advanced testing of ICT tools, systems and processes, while less advanced testing is already covered by Article 24 of DORA. For TLPT, in line with the TIBER-EU framework, no further differentiation is envisaged.

26. However, competent authorities still have the option to require the largest, most significant and most advanced entities to go beyond the elements outlined in this RTS. This RTS is to be understood as the minimum requirements for conducting TLPTs under DORA.

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

27. 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 on 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.

28. Given the wide scope of DORA, and the above-mentioned criteria, the proposed RTS introduces a two-layered approach. Financial entities operating in core financial services subsectors and playing a systemic role, such as CCPs and CSDs, as well as certain credit institutions[2], payment institutions, electronic money institutions, trading venues[3] and insurance and reinsurance undertakings, subject to fulfilling certain criteria or crossing quantitative thresholds, are required to perform TLPTs by default.

29. Further to the public consultation, the selection criteria applicable to insurance and reinsurance undertakings has been revised to make it more transparent for the market stakeholders. The thresholds applicable to payment institutions and electronic money institutions have been increased. The categories of financial instruments to be considered for the determination of thresholds in relation trading venues (equity or equity-like financial instruments, or bonds and other forms of securitised debts, or derivative contracts, or other non-equity financial instruments) have been mapped to the corresponding legal categories.

30. However, in order to reflect all aspects of the given mandate, TLPT authorities are given the possibility, based on an assessment of the above-mentioned impact-related, systemic character and ICT maturity-related factors, to opt-out some of these financial entities from the requirement to perform TLPT.

31. 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*."[4]), 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.

[2] Credit institutions in scope of TLPT are all individual legal entities authorised as a credit institution that are 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 or as other systemically important institutions (O-SIIs) or that are part of a G-SII or O-SII.

[3] In respect of trading venues, the required data on their market shares in the trading of various financial instruments would be provided by ESMA.

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

32. The majority of respondents agreed in principle with the two-layered approach. A number of them voiced the concern that belonging to a group structure was not sufficiently considered. This was incorporated into the text as much as possible: the belonging to a group shall be considered by the TLPT authority in the identification of a financial entity if common ICT systems or same ICT intra-group service provider are used.

33. However, ultimately, the identification must take place at the level of the financial entity. It is also true for credit institutions, which are identified individually, i.e. at legal entity level, based on their belonging to G-SIIs or O-SIIs. This means that all legal entities authorised as credit instutions and belonging to G-SIIs or O-SIIS are required to perform TLPT (unless opted-out by their TLPT authority).

34. This does not prevent TLPT authorities from deciding to conduct a test at group level through pooled or joint TLPTs, by involving several financial entities required to perform a TLPT and using the same ICT service provider or common ICT systems.

2.5 Approach on the testing: scope, methodology, conclusion

35. 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.

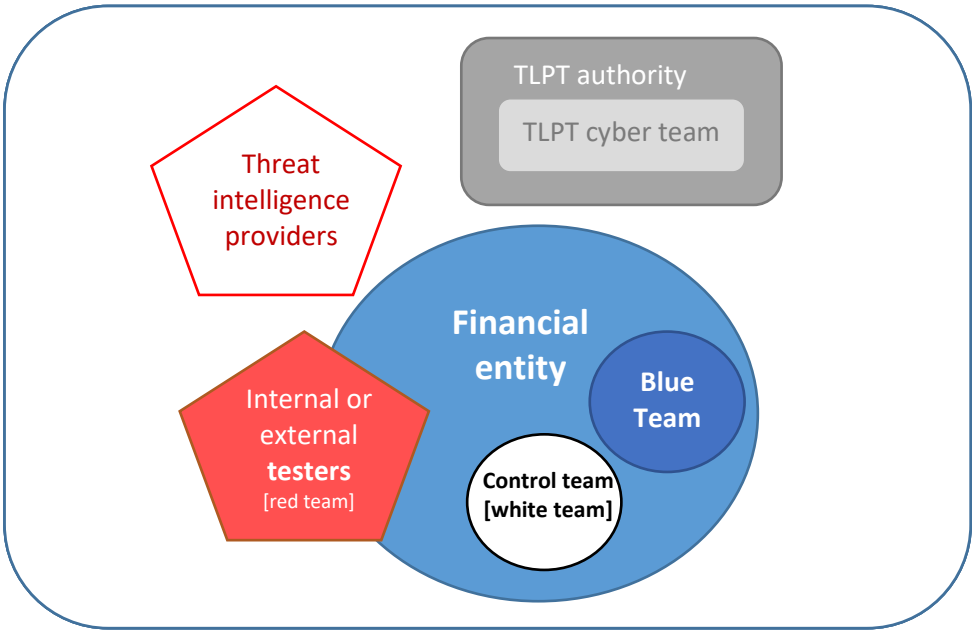
36. Nevertheless, some elements had to be altered owing to the different legal nature of a voluntary TIBER-EU Framework and a legally binding regulation. In general, the level of detail included in the TIBER-EU framework goes significantly beyond what can be replicated in an RTS.

37. 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.

38. The public consultation did not reveal any additional aspects from the TIBER process that should be included. In some instances respondents requested more guidance and best practices. Best practices by nature should not be legally binding and hence cannot be included in the RTS. However, the TIBER-EU framework and its numerous national implementations remain available for entities who wish for more detailed guidance and best practices.

2.5.1 Testing methodology

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



40. 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).

41. **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.

42. Respondents to the public consultation outlined that more clarity was needed on how risk management should be carried out for joint tests and pooled tests. For this reason a new article was introduced which clearly outlines that each financial entity is responsible for the management of its own risks and that the designated financial entity is responsible for identifying all common sources of risks that may emerge while all other financial entities are required to cooperate in the identification and mitigation of these risks.

43. A key way to minimize risk associated with TLPT and which is fully part of the approach to be followed to conduct 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.

44. 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.

45. Under DORA requirements for testers are laid out in Article 27 of 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.

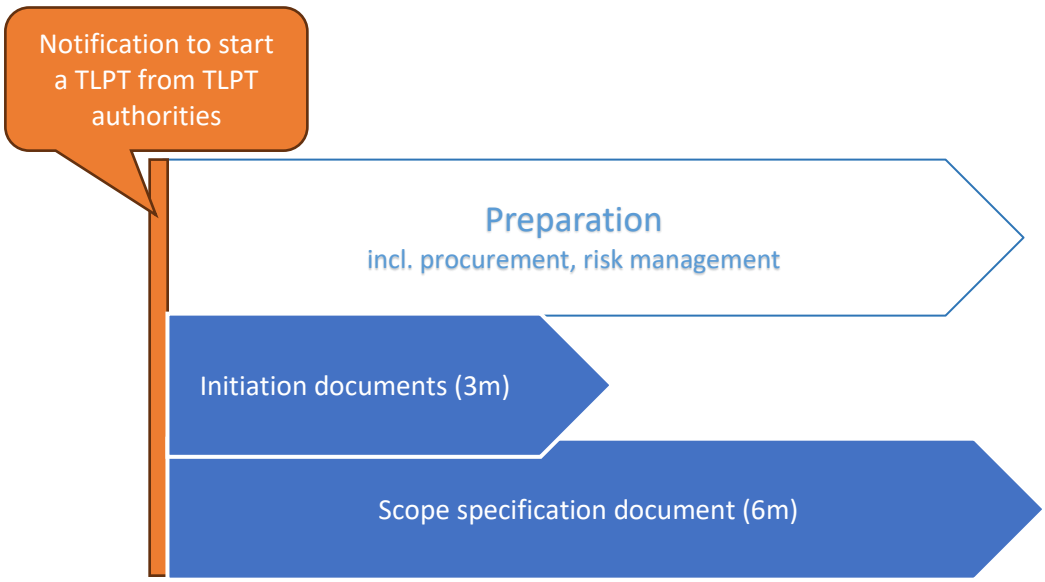
46. There were many comments in the public consultation outlining that the requirements will significantly limit the number of available testers and threat intelligence experts in what is a relatively young market. However, given the invasive and sensitive nature of TLPT a simple reduction in the number of years required would equally not be desirable. Acknowledging the respondents' concerns the draft RTS now includes the possibility that financial entities can procure providers who do not comply with some of the requirements, provided that they mitigate any additional risk this introduces. Further, the requirements have been relaxed in the sense that the experience now has to be in "penetration testing and red teaming" rather than in "threat intelligence led red-team tests".

2.5.2 Testing process

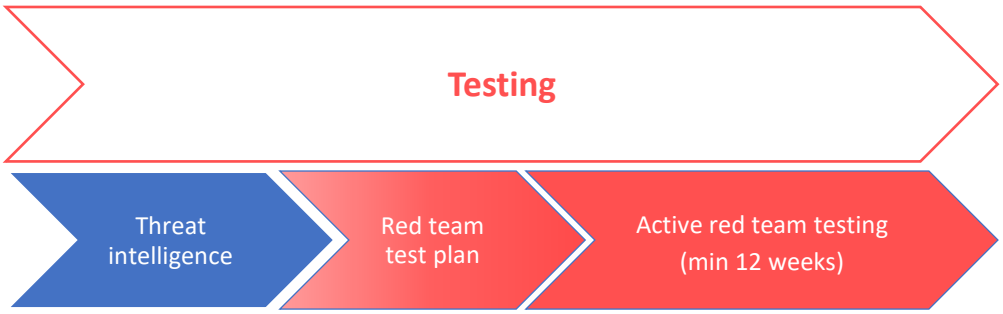
47. The process established in the proposed RTS very closely follows the TIBER-EU testing process sequence of phases, as follows:

48. 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.

49. A key factor in the success of a TLPT process is to anticipate the performance of the actual test as much as possible. First, the TLPT authorities should anticipate to the financial entities that they will be required to perform TLPT, by notifying this requirement as soon as possible before notifying the start of the actual TLPT. Authorities should also use this opportunity to ask financial entities to designate a contact person to receive any further notifications in relation to TLPT, to ensure the confidentiality of the test. Further, financial entities are strongly encouraged start liaising with threat intelligence providers and testers (for testers, assessing their internal resources) before being notified of the start of the actual TLPT and actually, as early as possible after acknowledging that they are in scope of the requirement to perform TLPT under Article 26 of DORA.



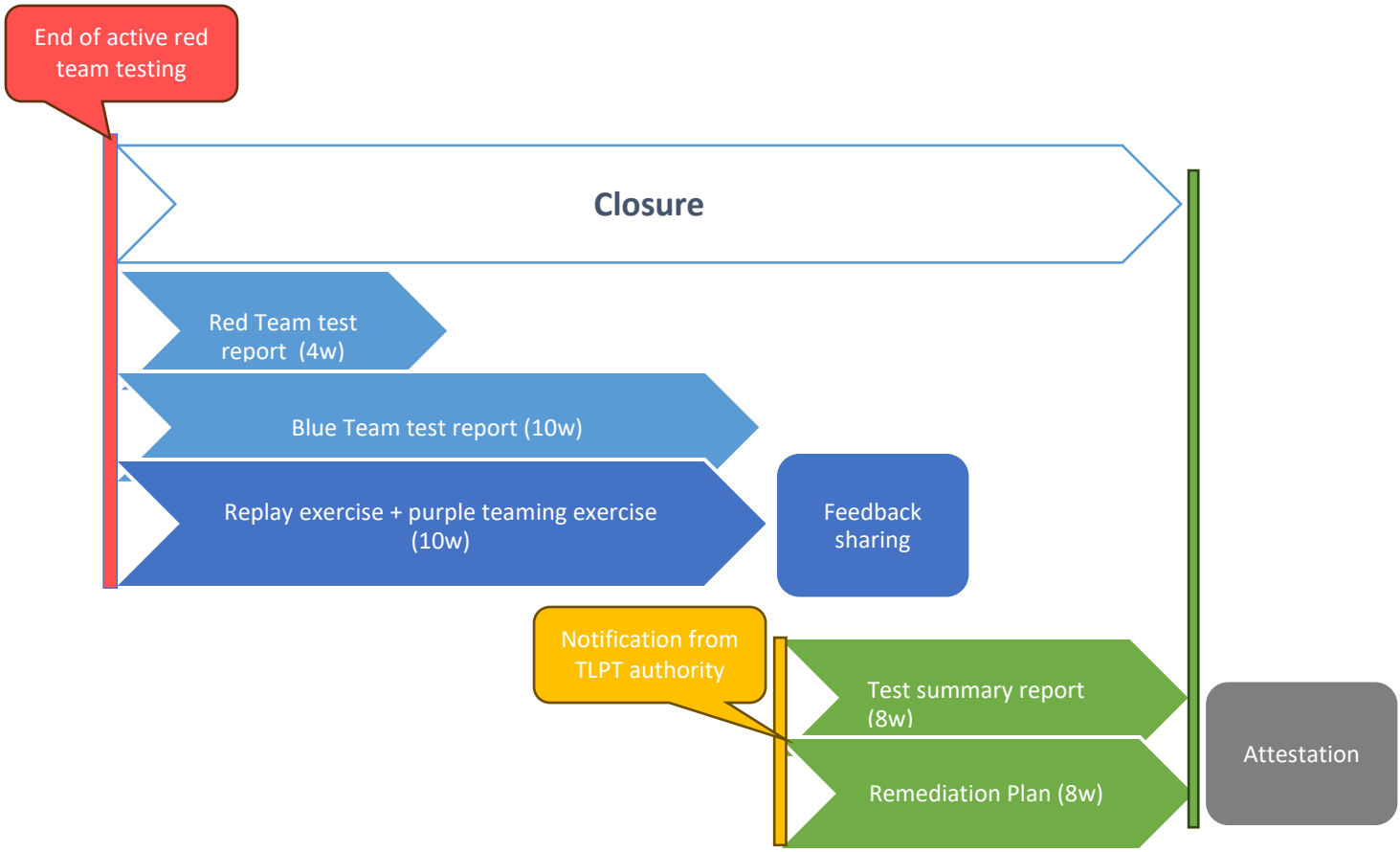
50. The **testing phase** also closely resembles the process described in the TIBER-EU framework. It is broken down into a threat intelligence part, which ultimately produces the scenarios, which are to be tested during the red teaming part of the testing phase. The active red teaming test has to be a minimum of 12 weeks. This 12-week duration is needed to mimic stealthy threat actors. It should be noted that the exact duration of each test will be fine-tuned in agreement with the TLPT authorities, in consideration of the specific characteristics of each TLPT (e.g. the specificties of the financial entity itself or whether the test involves an ICT service provider or several financial entities).



51. The **closure 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 also take place then, and ultimately a test summary report and remediation plan will be prepared by the financial entity and shared with the TLPT authority.

52. In respect of the **purple teaming exercise**, which was not mandatory in the original version of the TIBER-EU framework, clarifications have been brought in the recitals, definitions and articles of the draft RTS to address concerns raised by respondents to the public consultation as to when it should be carried out by the parties (i.e. if necessary to continue the TLPT, during the red team testing phase, and in any case, during the closure phase) and how.

53. Finally, the TLPT authority will issue an **attestation** that the TLPT was carried out in accordance with this regulation, identifying which critical or important functions were in scope of the TLPT.



54. The public consultation revealed that a number of respondents had concerns with regard to very tight deadlines, in particular during the closure phase. The drafting of blue team test report and remediation plans in particular are likely to require more time than the draft RTS permitted. As a result more time and flexibility has been introduced in the closure phase. It should also be reminded that each test will be organised on a case-by-case basis, and that the TLPT authorities, when reviewing the timeline for each phase of the test, will also consider the specificities of the test – number and types of parties involved, circumstances, etc.

55. **Pooled testing and joint testing**. Under DORA[5] 'pooled testing' designates a case where several financial entities will participate in a TLPT, for which an 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:

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

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.

56. Specific requirements relating to pooled testing have been introduced regarding the remediation plan (Article 13), the cooperation of TLPT authorities (Article 14(2)) and the attestation (Article 15(5)).

57. In addition to the "pooled testing", the draft RTS also clarifies the concept of "**joint testing**" which refers to a test, other than a pooled test, involving several financial entities using the same ICT intra-group service provider, or belonging to the same group and using common ICT systems. The criteria under which a pooled test (see above) can be used are quite restrictive and in practice there could be many more joint tests which do not fulfil the criteria of a pooled test.

58. From the respondents to the public consultation, it is evident that there were a number of misunderstandings with regard to what constitutes a pooled test. The newly introduced joint test actually corresponds to what many respondents considered to be pooled tests.

59. It has also been specified that in case a pooled test or a joint test is conducted, all scenarios shall relate to the financial entities' critical or important functions but at least one attack scenario shall concern the ICT service provider's system supporting those functions and other attack scenarios shall concern the financial entities' systems. This aims at ensuring that no financial entity remains untested for too long.

60. Finally, more has been added on the roles of TLPT authorities in the launch and conduct of such joint tests or pooled test in the supervisory cooperation section.

2.6 Approach on the use of internal testers

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

62. The possibility introduced currently in DORA to use internal testers is justified "in order to take advantage of internal resources available at corporate level"[6]. 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.

63. 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.

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

However, the possibility to use internal testers, is expected to be added in future revision of the TIBER-EU framework.

64. 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.

65. 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. These are requirements[7] 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.

66. 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 upon every third test[8]. As a second set of safeguards, the following requirements apply the use of internal testers[9]: prior supervisory approval, the absence of conflicts of interest within the financial entity and the mandatory use of an external threat intelligence provider.

67. 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.

68. The proposed additional requirements for the financial entity are to:
    (a) define a policy for the management of internal testers in TLPTs;
    (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.

[7] Article 27(1) of DORA

[8] 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."

[9] Article 27(2) of DORA

69. 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.

70. 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).

71. 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[10] of the financial entity shall also be considered as an internal tester.

72. There were a number of comments in the public consultation that asked for the requirements for internal testers to be aligned with those of external testers. This had always been the intention and the updated RTS uses clearer language in that regard. Additionally, the requirement for internal testers to have two year tenure at the financial entity has been lowered to one year. This is to address the concern outlined by many respondents to the public consultation that this requirement may be difficult to fulfil in a fast moving industry, while making the difference with external testers.

2.7 Approach on cooperation

73. 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*."

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

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

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

76. 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, so this would fall under the Joint TLPTs case below.

77. In such a first case (freedom to provide services in other Member States, including through branches), 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 on that TLPT, as observer, to assigning a test manager to that TLPT.

78. **Joint TLPTs**. 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 using the same ICT intra-group service provider, or belonging to the same group and using common ICT systems.

79. In such a 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.

80. **Pooled TLPTs**. The final case for cooperation between TLPT authorities is when pooled tests are carried out according to Article 26(4) of DORA. In this case the TLPT authorities shall designate which financial entity shall be the designated financial entity according to Article 26(4) DORA and which financial entities only participate in the pool and once again the TLPT authorities of the pariticipating financial entities shall agree amongst themselves as to who shall lead the TLPT.

81. Further to comments received during the public consultation, a clearer distinction has been made between pooled TLPT on one side, and joint TLPTs, on the other. To this end, a definition for 'joint TLPTs' has been introduced and the respectives provisiosn have been separated.

82. In addition, respondents to the public consultation had many suggestions to how supervisory cooperation could be improved which proved to be outside of the ESAs mandate.

~

3. 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[11], 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, or one of its national implementations, in as much as that framework or implementation 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 in the financial sector responsible for TLPT-related matters at national level according to Article 26(9) of Regulation (EU)

11 OJ L 333, 27.12.2022, p. 1.

2022/2554 should 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 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 should remain the authority for those TLPT-related tasks that have been not delegated.

(3) Considering the complexity of the TLPT and the risks relating to it, the test should be performed only by financial entities for which it is justified. Hence, authorities responsible for TLPT matters (TLPT authorities, either at national or Union level) should exclude from the scope of TLPT those financial entities operating in core financial services subsectors for which a TLPT is not justified. It means that credit institutions, payment and electronic money institutions, central security depositories, central counterparties, trading venues, insurance and reinsurance undertakings, even though when meeting the quantitative criteria identified in this Regulation, could be opted out of the TLPT scope in light of an overall assessment of their ICT risk profile and maturity, impact on the financial sector and related financial stability concerns.

(4) TLPT authorities should assess, in light of an overall assessment of the ICT risk profile and maturity, of the impact on the financial sector and related financial stability concerns, whether any type of financial entity other than credit institutions, payment institutions, electronic money institutions, central counterparties, central securities depositories, trading venues, insurance and reinsurance undertakings should be subject to TLPT. The assessment of the abovementioned qualitative elements should aim at identifying financial entities for which the TLPT is appropriate by using cross-sector and objective indicators. At the same time, the assessment of these elements should limit the entities subject to TLPT to those for which the test is justified. These elements should also be assessed with reference to new market participants (such as crypto asset service providers referred to in Title V of Regulation (EU) 2023/1114) which might have a more important role for the financial sector in the future.

(5) Where financial entities have the same ICT intra-group service provider or where they belong to the same group and rely on common ICT systems, it is important that TLPT authorities consider the structure and its systemic character or importance for the financial sector at national or Union level in the assessment of whether a financial entity should be subject to TLPT and of whether the TLPT should be conducted at entity level or at group level (through a joint TLPT).

(6) In order to mirror the TIBER-EU framework, it is necessary that the testing methodology provides for 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 (mirroring the TIBER-EU '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 (the latter mirroring the TIBER so-called 'red team provider').

(7) 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, it should be ensured 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. Hence, the TLPT cyber teams should include test managers responsible for overseeing the individual TLPTs and be responsible for planning and coordination of individual tests. TLPT cyber teams should serve as single point of contact for test-related communication to internal and external stakeholders, collect and process feedback and lessons learned from previously conducted tests and provide support to financial entities undergoing TLPT testing.

(8) To mirror the TIBER-EU framework methodology, 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, to safeguard the confidentiality of tests, and unless they have resources or expertise 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.

(9) It is important, for consistency with the TIBER-EU framework, that the TLPT authority closely follows the test in each of its stages. Considering the nature of the test and the risks associated to it, it is fundamental that the approach to be followed for each specific phase of the testing refers, where relevant, to the role of the TLPT authority. In particular, the TLPT authority should be consulted and should validate those assessments or decisions of the financial entities that may, on the one hand, have an effect on the effectiveness of the test and, on the other hand, have an impact on the risks associated with the test. Examples of the fundamental steps on which a specific involvement of the TLPT authority is necessary include the validation of certain fundamental documentation of the test, the selection of threat intelligence providers and testers and risk management measures. The involvement of the TLPT

authority, with particular reference to validations, should not result in an excessive burden for the authorities and should therefore be limited to those documentation and decisions directly affecting the positive outcome of the TLPT. The involvement of the TLPT authority as described in this Regulation is also necessary for the purposes of the issuance of the attestation pursuant to Article 26(7) of Regulation (EU) 2022/2554. Through the active participation to each phase of the testing the TLPT authorities may effectively assess compliance of the financial entities with the relevant requirements.

(10) 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.

(11) 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.

(12) 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, without prejudice to the internal processes of the financial entity and the responsibility and delegations already provided to the control team lead,

information or, in particular cases, approval of the TLPT risk management measures by the financial entity's management body itself may be appropriate. It is also 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 and to reduce the abovementioned risks.

(13) 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. This Regulation establishes comprehensive criteria for testers, both internal and external, and threat intelligence providers, always external. In case the threat intelligence provider and the external testers are part of the same company, the staff assigned to the test should be adequately separated. Acknowledging the evolving state of this market, there may be exceptional circumstances where financial entities are unable to secure suitable providers who meet these standards. Therefore, financial entities, upon evidencing the unavailability of fully compliant and suitable providers, should be permitted to engage those who do not satisfy all criteria, conditional upon the proper mitigation of any resultant additional risks and to an assessment of all these elements by TLPT authority.

(14) When several financial entities and several TLPT authorities are involved in a TLPT, the roles of all parties in the TLPT process should be specified to conduct the most efficient and safe test. For the purposes of pooled testing, specific requirements are necessary to specify the role of the designated financial entity, and namely that it should be in charge of providing all necessary documentation to the lead TLPT authority and monitoring the test process. The designated financial entity should also be in charge of the common aspects of the risk management assessment. Notwithstanding the role of the designated financial entity, the obligations of each financial entity participating to the pooled TLPT process remain unaffected during the pooled test. The same principle is valid for joint TLPTs.

(15) As evidenced by the experience of the implementations of the TIBER-EU framework, holding in-person or virtual meetings including all relevant stakeholders (financial entities, 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.

(16) In order to ensure the smooth performance of the TLPT, the TLPT authority should clearly present its expectations with respect to the test to the financial entity. In that respect, the test managers 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.

(17) The financial entity should select the critical or important functions that will be in scope of the TLPT based on various criteria relating to the importance of the function for the financial entity itself and the financial sector, at national and at Union level, not only in economic terms but also considering for instance the symbolic or political status of the function. If the testers and threat intelligence provider are not involved during the scoping process, the control team should provide them with detailed information on the agreed scoping, to facilitate a smooth transition to the phase of threat intelligence gathering.

(18) 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. Based on the TIBER-EU framework application, the threat intelligence gathering process is typically lasting approximately four weeks.

(19) It is essential that, prior to the red team testing phase of the TLPT, the testers receive detailed explanations on the targeted 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 threat intelligence report to finalise the red team test plan.

(20) 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. On the basis of the experience gathered with the TIBER-EU framework, the time allocated should be at least twelve weeks and be determined taking into account the number of parties involved, the TLPT scope, the resources of the involved financial entity or entities, any external requirements and the availability of supporting information supplied by the financial entity.

(21) 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).

(22) 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'. Leg-ups can broadly be categorized in information and access leg-ups and may for instance consist of the provision of access to ICT system or internal networks to continue with the test and focus on the following attack steps.

(23) During the active red teaming in the testing phase, purple teaming activities should be used as a last resort in exceptional circumstances and once all alternative options have been exhausted. In the context ofthis limited purple teaming exercise, the following methods can be used: "catch-and-release", where testers attempt to continue the scenarios, get detected and then resume the testing again; "war gaming", which allows for more complex scenarios to test strategic decision making; or "collaborative proof-of-concept" which allows testers and blue team members to jointly validate specific security measures, tools, or techniques in a controlled and cooperative environment.

(24) The TLPT should be 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. For this purpose and to allow for adequate preparation, the red team test report and the blue team test report should be made available to all parties involved in the replay activities, prior to conducting any replay activities. Additionally, a purple teaming exercise, in the closure phase, should be carried out to maximize the learning experience. Methods that may be used for purple teaming in the closure phase include discussions of alternative attack scenarios, exploration on live systems of alternative scenarios or the re-exploration of planned scenarios on live systems that the testers had been unable to complete or execute during the testing phase.

(25) 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.

(26) 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.

(27) 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.

(28) 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.

(29) The European Supervisory Authorities have 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[12], 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[13] 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[14],

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, where relevant in consideration of the scope of the TLPT, staff of its third-party service providers and any other party, who 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, where relevant, staff of the financial entity’s third-party service providers and any other party deemed relevant in consideration of the scope of the TLPT, of the financial entity’s third-party service providers, that are defending a financial entity's use of network and

[12] 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).

[13] 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).

[14] 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).

information systems by maintaining its security posture against simulated or real attacks and that is not aware of the TLPT;

(4) 'blue team tasks' means tasks that are typically carried out by the blue team such as security operation centre (SOC), ICT infrastructure services, helpdesk services, incident management services at operational level;

(5) 'purple teaming' means a collaborative testing activity that involves both the testers and the blue team;

(6) 'TLPT authority' means:

(a) the single public authority in the financial sector designated in accordance with Article 26(9) of Regulation (EU) 2022/2554, or

a. the authority in the financial sector 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

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

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

(8) '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;

(9) 'threat intelligence provider' means the expert(s), external to the financial entity and to ICT intra-group service providers if any, 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;

(10) '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, and where no other reasonable alternative exists, including for insufficient time or resources in a given TLPT;

(11) '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;

(12) '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;

(13) ‘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 financial entity and its ecosystem would it fall in the hands of malicious actors;

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

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

(16) ‘joint TLPT’ means a TLPT, other than a pooled TLPT referred to in Article 26(4) of Regulation (EU) 2022/2554, involving several financial entities using the same ICT intra-group service provider, or belonging to the same group and using common ICT systems.

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 [15] 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 150 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[16].

(c) Electronic money institutions, exceeding in each of the previous two financial years EUR 150 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) the trading venue with the highest market share in terms of turnover at national level in each of the preceding two financial years in one or more of the following:

—transferable securities as defined in point (44)(a) of Article 4(1) of Directive 2014/65/EU of the European Parliament and of the Council[17];

—transferable securities as defined in point (44)(b) of Article 4(1) of Directive 2014/65/EU;

—derivatives as defined in Article 2(1)(29) of Regulation (EU) No 600/2014 of the European Parliament and of the Council[18];

—structured finance products as defined in Article 2(1)(28) of Regulation (EU) No 600/2014 ;

- emission allowances as defined in point (11) of Section C of Annex I to Directive 2014/65/EU;

[15] 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).

[16] 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).

[17] Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (recast) (OJ L 173 12.6.2014, p. 349).

[18] Regulation (EU) No 600/2014 of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Regulation (EU) No 648/2012 (OJ L 173 12.6.2014, p. 84).

(ii) the trading venue whose market share in terms of turnover at Union level exceeds 5% in each of the preceding two financial years in one or more of the following:

—transferable securities as defined in point (44)(a) of Article 4(1) of Directive 2014/65/EU[19],

—transferable securities as defined in point (44)(b) of Article 4(1) of directive Directive 2014/65/EU,

—derivatives as defined in Article 2(1)(29) of Regulation (EU) No 600/2014,

—structured finance products as defined in Article 2(1)(28) of Regulation (EU) No 600/2014;

- emission allowances as defined in point (11) of Section C of Annex I to Directive 2014/65/EU;

For the purposes of point (ii) of this point (f), where the trading venue is part of a group using common ICT systems or the same ICT intra-group service provider, the turnover of the securities and derivatives contracts on all trading venues pertaining to the same group and established in the Union shall be considered.

(g) Insurance and reinsurance undertakings that meet all the following criteria:

(i) gross written premium (GWP) exceeding EUR 1 500 000 000;

(ii) technical provisions exceeding EUR 10 000 000 000;

(iii) in case of life insurance undertakings, as referred to in Article 13, point (1), of Directive 2009/138/EC of the European Parliament and of the Council[20], and of insurance undertakings pursuing both life and non-life activities, total assets exceeding 3.5% 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.

TLPT authorities shall create a subset of all insurance and reinsurance undertakings by applying the criteria listed in the first subparagraph. Insurance and reinsurance undertakings included in this subset shall be required to perform TLPT where they also meet one or more of the following criteria:

(i) gross written premium (GWP) exceeding EUR 3 000 000 000;

(ii) technical provisions exceeding EUR 30 000 000 000;

(iii) total assets exceeding 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.

[19] Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (recast) (OJ L 173 12.6.2014, p. 349).

[20] Directive 2009/138/EC of the European Parliament and of the Council of 25 November 2009 on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II) (recast) (OJ L 335, 17/12/2009, p. 1).

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 4 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 TLPT.

3. Where more than one financial entity belonging to the same group and using common ICT systems, or where more than one financial entity using the same ICT intra-group service provider meet the criteria set out in points (a) to (g) of paragraph 1, the TLPT authorities of these financial entities shall decide if the requirement to perform TLPT on an individual basis is relevant for these financial entities, in accordance with Article 14(2). Where the TLPT authority of the parent undertaking of such group is different from the TLPT authority(ies) of the financial entities referred to in the first subparagraph, it shall be consulted.

4. TLPT authorities shall assess whether any financial entities other than those referred to in paragraph 1 shall be required to perform TLPT, taking into account their impact, systemic character and ICT risk profile, assessed on the basis of all of the following criteria:

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

      (i) 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;

      (ii) the extent and nature of the interconnectedness of the financial entity with other financial entities in the financial sector at national and Union level;

      (iii) the criticality or importance of the services provided to the financial sector;

      (iv) the substitutability of the services provided by the financial entity;

      (v) 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;

      (vi) 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:

(i) the risk profile of the financial entity;

(ii) the threat landscape of the financial entity;

(iii) the degree of dependence of critical or important functions or their supporting functions of the financial entity on ICT systems and processes;

(iv) the complexity of the ICT architecture of the financial entity;

(v) 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;

(vi) outcomes of any supervisory reviews relevant for the assessment of the ICT maturity of the financial entity;

(vii) the maturity of ICT business continuity plans and ICT response and recovery plans;

(viii) 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;

(ix) 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, a test manager and at least one alternate shall be designated.
3. The test managers shall monitor and ensure that the requirements laid out in this Regulation are complied with.
4. The contact details of the TCT shall be communicated to the financial entity through the notification referred to in Article 8(1).
5. The TLPT authority shall participate to all the phases of the TLPT and shall endeavour to provide feedback, validations or approvals in a period of time adequate to expediently carry out the TLPT.

Article 4

Organisational arrangements for financial entities

1. Financial entities shall appoint a control team lead who shall be responsible for the day-to-day management of the TLPT 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 provides any information pertaining to the TLPT to the test managers upon request;

(f) where possible, parties involved in the TLPT refer to it by code name only.

Article 5

Risk management for TLPT

1. During the preparation phase referred to in Article 8, 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, for each TLPT:

(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 provides at least three references from previous assignments in the context of penetration testing and red team testing;

(d) the external testers provide at least five references from previous assignments related to penetration testing and red team testing;

(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 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 in threat intelligence in the context of penetration testing and red team testing;

iv. not simultaneously perform any blue team tasks or other services that may present a conflict of interest with respect to the financial entity, ICT third-party service provider or an ICT intra-group service provider involved in TLPT to which they are assigned;

v. be separated from and not reporting to staff of the same provider providing external testers for the same TLPT;

(f) for external testers, the staff of the red team assigned to the TLPT shall:

i. be composed of at least a manager, with at least five years of experience in penetration testing and red team testing as well as at least two additional testers, each with penetration testing and red team testing 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 penetration testing and red team testing.;

iv. not be employed by, nor provide services to, a provider that simultaneously performs blue team tasks for a financial entity, ICT third-party service provider or an ICT intra-group service provider involved in the TLPT;

v. be separated from any staff of the same provider simultaneously providing threat-intelligence services for the same TLPT.

(g) the testers and the threat intelligence provider shall 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 accounts 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 (g), 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 of the blue team activities and information to the control team of any possible detections; and

(i) 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.

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

   In exceptional circumstances, financial entities may contract external testers and threat intelligence providers that are not meeting one or more of the requirements listed in points (a) to (f) of paragraph 2, provided that they adopt appropriate measures to mitigate the risks relating to the lack of compliance with such points and record them.

4. In the performance of risk assessment and management, the control team shall at least consider the following types of risks related to:

   (a) granting access to threat intelligence provider and external testers, where applicable, to sensitive information and confidential information on the financial entity;

   (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 due to the activities of the testers and potential impacts on third parties;

(e) blue team activity, including risks related to interruption of critical activities and corruption of data due to the activities of the blue team and potential impacts on third parties;

(f) incomplete restoration of systems affected by the TLPT.

Article 6

Risk management for pooled and joint TLPTs

1. In the case of a joint TLPT or a pooled TLPT, the control team of each financial entity shall conduct its own risk assessment and establish its own risk management measures.

2. The control team of the designated financial entity referred to in Article 14(3)(b) or in Article 26(4) of Regulation (EU) 2022/2554 shall consider, in conducting the risk assessment, aspects relating to the involvement in the TLPT of multiple financial entities. The control teams of the involved financial entities shall cooperate to identify potential joint risks.

Section II

Testing Process

Article 7

Specificities for pooled and joint TLPTs

1. Unless otherwise decided by the lead TLPT authority, where several financial entities, selected according to Article 14(2) or 14(4) are involved in a TLPT, each financial entity shall follow each of the steps described in Articles 8 to 13.

2. Unless otherwise provided in this Regulation, where several TLPT authorities are involved in a joint TLPT or in a pooled TLPT, references in Articles 8 to 13 to the

"TLPT authority" shall be understood as a reference to the lead TLPT authority for such pooled or joint TLPT, as referred to in Article 14(3) or 14(5).

Article 8

Preparation phase

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

   (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. Where the documents referred to in points (a) to (e) of paragraph 1 are complete and ensure the suitability and effective performance of the TLPT, the TLPT authority shall validate the TLPT initiation documents of the financial entity and notify the latter thereof.

3. Following the validation of the TLPT initiation documents by the TLPT authority, the financial entity shall set up a control team to 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. Where the TLPT authority considers that the initial composition of the control team and any subsequent changes to it are adequate for the performance of the tasks referred to in paragraph 3, the TLPT authority shall validate the control team and notify the control team lead thereof.

5. The financial entity shall submit a scope specification document containing all information set out in Annex II to the test managers 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.

6. 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) where available, threat intelligence concerning the function.

7. 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.

8. The financial entity shall ensure that the procurement or assignement of testers and threat intelligence providers is completed prior to the initiation of the testing phase.

9. Prior to the initiation of the testing phase, the control team shall consult the test managers on the TLPT risk assessment and on the risk management measures. The control team shall review the risk assessment or the risk management measures where the TLPT authority assesses that they do not adequately address the risks of the TLPT.

10. The control team shall assess the compliance of threat intelligence providers and 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 and document the

outcome of this assessment. The control team shall select provider(s) in accordance with this assessment and its risk management practices. Prior to contracting the selected threat intelligence provider and external tester, the control team shall provide evidence of compliance to the test managers. The control team shall not proceed with contracting the selected threat intelligence provider and external testers where the TLPT authority assesses that the selected threat intelligence providers and external testers do not ensure compliance with, where appropriate, national security legislations or Article 5(2), or when the financial entity does not comply with Article 5(3), first subparagraph, or when the circumstances described in Article 5(3), second subparagraph, are not met.

11. Where the scope specification document is complete and ensures the performance of an appropriate and effective TLPT, the TLPT authority shall inform the control team lead of its validation thereof.

Article 9

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 existing 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 lead 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. No more than one of the selected scenarios may be non-threat-led and may 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 concerning the financial entity.

   For pooled TLPTs, without prejudice to the scenarios targeting directly the critical or important functions of the financial entities involved in the test, at least one scenario shall include the ICT third-party services provider's relevant underlying ICT systems, processes and technologies supporting the critical or important functions of the financial entities in scope.

   Where the test is a joint TLPT involving an ICT intra-group service provider, without prejudice to the scenarios targeting directly the critical or important functions of the financial entities involved in the test, at least one scenario shall include the ICT intragroup services provider's relevant underlying ICT systems, processes and technologies supporting the critical or important functions of the financial entities in scope.

5. The threat intelligence provider shall provide the targeted threat intelligence report to the control team, including the scenarios selected according to paragraphs 2 to 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 test manager for approval. Where the targeted threat intelligence report is complete and ensure the performance of an effective TLPT, the TLPT authority shall inform the control team lead of its approval thereof.

Article 10

Testing phase: Red Team Test

1. Following approval of the targeted 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. Where the red team test plan is complete and ensure the performance of an effective TLPT, the TLPT authority shall inform the control team lead of its 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 TLPT scope, to the scale, activity, complexity and number of the financial entities and ICT third-party or ICT intragroup service providers involved in the TLPT, and in any case shall last for at least twelve weeks. Attack scenarios may be executed in sequence or at the same time. The control team, the threat intelligence provider, the testers and the test managers 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 lead and the test managers.

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 test managers.

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 or ICT intragroup service provider, 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 while ensuring its secrecy to the test managers for validation.

10. Under exceptional circumstances triggering risks of impact on data, damage to assets, and disruption to critical or important functions, services or operations of the financial entity itself, of its ICT third-party service providers or ICT intragroup services providers, or disruptions to its counterparts or to the financial sector, the control team lead may suspend the TLPT, or, as a last resort, 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. The duration of the limited purple teaming exercise shall be counted for the purpose of the twelve week minimum duration of the active red team testing phase.

Article 11

Closure phase

1. Following the end of the active red team testing phase, the control team lead 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.

   At the request of the test managers, the report referred to in the first subparagraph of this paragraph shall not contain sensitive information.

4. Upon receipt of the red team test report, and no later than ten weeks after the end of the active red team testing phase, 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.

   At the request of the test managers, the report referred to in the first subparagraph of this paragraph shall not contain sensitive information.

5. No later than ten weeks after the end of the active red team testing phase, the blue team and the testers shall carry out a replay of the offensive and defensive actions performed during the TLPT. The control team shall also 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 managers may provide feedback.

7. Once the TLPT authority has notified the control team lead that it has assessed that the blue team test report and the red team test report contain the information set out in Annex V and Annex VI, the financial entity shall within eight weeks submit the report summarizing the relevant findings of the TLPT referred to in Article 26(6) of Regulation (EU) 2022/2554, containing the elements set out in Annex VII for approval.

At the request of the TLPT authority, the report referred to in the first subparagraph of this paragraph shall not contain sensitive information.

Article 12

Remediation plan

1. Within eight weeks from the notification referred to in Article 11(7), 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.

CHAPTER IV

REQUIREMENTS AND STANDARDS GOVERNING THE USE OF INTERNAL TESTERS

Article 13

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 internal 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 12 months;

      iii. include provisions on training on how to perform penetration testing and red team testing 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 8;

   (b) the red team test report referred to in Article 11(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 14

Cooperation

1. For the purposes of conducting a TLPT in relation to a financial entity providing services in more than one Member State, including through a branch, its TLPT authority shall:

   (a) determine which TLPT authorities in host Member States shall 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 TLPT;

   (c) unless otherwise agreed by the TLPT authorities, the TLPT authority of the financial entity 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 test and adopt all the decisions necessary to carry out the TLPT appropriately and effectively. 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. Where a financial entity uses the same ICT intra-group service provider as financial entities established in other Member States, or belongs to a group and uses ICT systems common to financial entities of the same group established in other Member States, the TLPT authority of the financial entity shall contact the TLPT authorities of the other financial entities using the same ICT intra-group service provider or using the same ICT systems as part of the group and assess with them the feasibility and suitability of conducting a joint TLPT in their respect. A joint TLPT shall be preferred to an individual TLPT where it may result in reduction of costs and resources for the financial entities and for the TLPT authorities, provided that the soundness and efficacy of the test is not prejudiced.

3. For the purposes of conducting a joint TLPT:

   (a) the TLPT authorities of the financial entities shall agree on which financial entity shall be designated to conduct the TLPT, considering the group structure and the efficiency of the test;

(b) the TLPT authority of the financial entity designated in accordance with point (a) shall lead the TLPT, unless otherwise agreed by the TLPT authorities of the financial entities participating in the joint TLPT;

(c) the TLPT authorities of the financial entities other than the designated financial entity to lead the joint TLPT may either express their interest in following the TLPT as observers or assign a test manager for that TLPT. The lead TLPT authority shall coordinate all TLPT authorities involved in the joint TLPT and adopt all the decisions necessary to carry out the joint TLPT in a sound and effective way.

4. Where a financial entity intends to conduct a pooled TLPT as referred to in Article 26(4) of Regulation (EU) 2022/2554 possibly involving financial entities established in other Member States, its TLPT authority shall contact the TLPT authorities of the other financial entities and assess with them the feasibility and suitability of conducting a pooled TLPT in their respect in accordance with Article 26(4) of Regulation (EU) 2022/2554.

5. For the purposes of conducting a pooled TLPT as referred to in Article 26(4) of Regulation (EU) 2022/2554:

   (a) the TLPT authorities of the financial entities shall agree on which financial entity shall be designated to conduct the pooled TLPT, considering the ICT services provided by the ICT third-party service provider to the financial entities and the efficiency of the test;

   (b) the TLPT authority of the financial entity designated in accordance with point (a) shall lead the TLPT, unless otherwise agreed by the TLPT authorities of the financial entities participating in the pooled or joint TLPT;

   (c) the TLPT authorities of the financial entities other than the designated financial entity to lead the pooled TLPT may either express their interest in following the TLPT as observers or assign a test manager to that TLPT. The lead TLPT authority shall coordinate all TLPT authorities involved in the pooled TLPT and adopt all the decisions necessary to carry out the pooled TLPT in a sound and effective way.

6. 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.

7. The attestation referred to in Article 26(7) of Regulation (EU) 2022/2554 shall at least mention the information set out in Annex VIII.

8. Where several TLPT authorities have been involved in a TLPT, the attestation referred to in Article 26(7) of Regulation (EU) 2022/2554 shall be provided by the lead TLPT authority.

Article 15

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 8(1) point d) and 8(2) point a, 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 8	yyyy-mm-dd
(2) Testing Phase, in accordance with Articles 9 and 10	yyyy-mm-dd
(3) Closure Phase, in accordance with Article 11	yyyy-mm-dd
(4) Remediation plan in accordance with Article 12	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 targeted 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 or important 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;
    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(4).

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 to reconstruct the attack and to mitigate its effects;

(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 of the blue team test report

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

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 targeted threat intelligence report;

(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.

ANNEX VIII

Details of the attestation of the TLPT

The attestation referred to in Article 26(7) of Regulation (EU) 2022/2554 shall include at least the following information:

(a) on the performed TLPT:

a. the starting and end dates of the TLPT;

b. the critical or important functions in scope of the test;

c. where relevant, information on critical or important functions in scope of the test in relation to which the TLPT was not performed;

d. where relevant, other financial entities that were involved in the TLPT;

e. where relevant, the ICT third-party services providers that participated in the TLPT;

f. in respect of testers:

i. whether internal testers were used;

ii. whether Article 5(3), second subparagraph, was used by the financial entity;

g. the duration, in calendar days, of the active red team testing phase;

(b) where several TLPT authorities have been involved in the TLPT, the other TLPT authorities, and in which capacity;

(c) list of the documents examined by the TLPT authority for the purposes of the attestation.

4. 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 Final Report (FR) on the draft RTS specifying on certain aspects of advanced testing of ICT tools, systems and processes based on TLPT.

Problem identification

(3) Complexity of 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, 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 mentioned 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 draft RTS.

4.1 Policy issue 1: Consideration of group structures for the identification of financial entities required to perform TLPT

Options considered

(10) Financial entities can belong to corporate structures or financial groups, operating in several Member States or not. In such case, several financial entities might be using common ICT systems or the same ICT intra-group service provider. However, financial entities required to perform TLPT have to identified at the level of individual legal entities.

(11) Option A: The circumstance that a financial entity or several of them are part of a group that uses same common ICT systems or the same ICT intra-group service provider should 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(1) and are using the same common ICT systems, each such financial entity of that group might be required to perform a TLPT .

(12) Option B: Where several financial entities use the same ICT service intra-group provider or are part of a group and use common ICT systems or, the relevant TLPT authority or authorities should also consider this circumstancee corporate structure when identifying the financial entities to be required to perform a TLPT and be able to select the most relevant financial entities of that group.

Cost-benefit analysis

(13) If all of the financial entities using the same ICT intragroup provider, or belonging to a group and using common ICT systems, are required to perform a TLPT, this could lead to multiplication of TLPTs on financial entities presenting similar charteristics in terms of importance, systemic character and ICT maturity, and to be performed on the same ICT systems. The potential multiplication of TLPTs would bring duplication and limited benefits compared to the efforts of conducting numerous and complex tests (e.g. in joint form).

(14) Where TLPT authorities have to assess the relevance of requiring a financial entity to perform a test by considering also the fact that it belongs to a group a financial entities using the same ICT intra-group service provider or common ICT systems, the less relevant financial entities can be opted-out and resources can be better used.

Preferred option

(15) Option B is preferred.

4.2 Policy issue 2: approach for the identification

Options considered

(16) DORA has a wide scope, including different types of financial entities 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 the 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) Option A: In order to reflect the 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.

(19) Option B: 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.

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 features which might also be taken into account.

Preferred option

(21) Option B is preferred.

4.3 Policy issue 3: Additional Requirements on testers and threat intelligence providers

Options considered

(22) 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.

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

(24) Option B: Another option is to include the key quantitative requirements for testers and TI providers from the TIBER-EU Procurement Guidelines.

(25) Option C: A third option is to include slightly modified requirements which allow for some more flexibility while retaining most of the benefits of the quantitative criteria under TIBER.

Cost-benefit analysis

(26) 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.

(27) 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.

(28) 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.

(29) 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.

(30) 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.

(31) 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.

(32) 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 draft RTS.

Preferred option

(33) Option C is preferred. The draft RTS has introduced some flexibility into the quantitative criteria presented in the public consultation. The experience of testers no longer has to be exclusively limited to "intelligence led red teaming" but has been broadened to "penetration testing and red teaming". Further the possibility has been introduced to hire testers who do not fulfil all the criteria, provided that the financial entity identifies and mitigates all the additional risks this presents to the TLPT.

4.4 Policy issue 4: Pooled testing

Options considered

(34) Conducting a TLPT in the form of a pooled test is an option provided in Article 26(4) of DORA, for tests involving an ICT third-party services provider (ICT TPP) and several financial entities that use such ICT TPP, where certain specific conditions are fulfilled. So far not many TLPTs have been conducted as pooled tests and this type of test is not covered under the TIBER-EU framework developed by the ECB.

(35) Option A: not specifying anything on pooled testing in the draft RTS at this stage and waiting for a guidance ot be developed under the TIBER-EU framework.

(36) Option B: developing at least high-level RTs provisions allowing to operationalize the option provided in DORA to conduct TLPTs involving several financial entities and an ICT services provider.

Cost-benefit analysis

(37) The public consultation revealed a need for more guidance on pooled testing in particular, and in general on tests involving several financial entities and an ICT service provider.

(38) If nothing is specified in the draft RTS in this respect, there is a high risk of divergences between the national practices, while the ESAs consider this is fully part of their legislative mandate, as a specific type of TLPT calling for a particular methodology and process, as well as specific supervisory cooperation arrangements in case of cross-border exercises.

Preferred option

(39) Option B is preferred. Following the public consulation, various aspects og the draft RTS have been clarified in relation to pooled testing (in particular on risk management, process and supervisory cooperation in case of cross-border tests), but also in respect of joint tests.

5. Feedback from the ESAs' Stakeholders Groups

5.1 General comments

The Stakeholder Groups (SGs) welcome the opportunity to comment on the "Draft Regulatory Technical Standards specifying elements related to threat led penetration tests".

In our response, the SGs focus only on those elements that we feel competent enough to provide meaningful input.

ESAs response

The ESA welcome and take note of the feedback received from the ESA's SG.

5.2 Questions for consultation

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

The SGs agree, in principle, with the proposed approach, subject to the following observations:

The SGs note, that TIBER-EU has yet to publish comprehensive guidance for combined TLPTs with individual financial entities (FEs) and ICT third party providers (TPPs) (Article 26(3) DORA), or for pooled tests with multiple FEs or TPPs (Article 26(4) DORA). The RTS makes reference to these tests, as per the DORA Level 1 text, but does not provide further guidance concerning their operationalisation. Both forms of test involve a significant degree of complexity, with material legal, operational and practical challenges that have yet to become established norms within the financial or technology sectors. The financial entity, who would be accountable for administering both tests, would face significant risk if they were required by a TLPT authority to do a combined or pooled test. There is a risk that not all stages of the TLPT required by the RTS would be completed and the expected timelines set out in the RTS may not adequately account for the complexity of either test. Further guidance concerning combined or pooled TLPT tests should be obtained before such tests could be completed in practice.

Some members of the SGs note that the RTS introduces mandatory 'purple teaming', which is an optional element of TIBER-EU and not a stated requirement in DORA Level 1. They suggest that a mandatory 'purple team' exercise after an external test which indicated limited to no vulnerabilities would not add value to the external testing team or the FE. They recommend, therefore, that 'purple teaming' should only be required when a sufficient number of vulnerabilities are demonstrated in the 'red/blue teaming' exercise. Other members believe that there could be other situations where 'purple teaming' is not required and would recommend that it should be encouraged but made optional altogether.

ESAs response

The ESAs welcome the SGs' overall support for the cross-sectoral approach followed in the draft RTS.

On combined TLPTs with individual FEs and ICT TPPs and pooled tests, the ESAs have provided more details on the operationalisation of such TLPTs, definig the concept of 'joint TLPT' and including clarifications on how to manage a process for such tests on the side of the FEs (for instance, specifying that risk management should be made at entity level but that the designted FE shall carry it out for the joint or common aspects of the test) and on the side of the TLPT authorities (in the section on cooperation).

On purple teaming, the ESAs have clarified when such exercise shall be carried out (either during the red team phase, if it becomes necessary due to a detection buy the blue team, for instance, or if not diring the closure phase) in order to maximise the learning potential of TLPTs. The ECB confirmed that such exercise will be mandatory in next version of the TIBER-EU framework.

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

The SGs agree with the ESAs approach in general. Some members of the SGs believe that the RTS should allow for more flexibility in certain areas given the diverse set of financial entities covered by DORA and the fact that their existing capabilities and experience with TLPT may also differ widely. Article 2(1) RTS sets out the criteria for identifying FEs that would be in scope to complete TLPT under DORA. The SGs agree with the criteria, which are based on definitions and metrics used elsewhere in relevant sectoral legislation to identify 'significant' or 'systemically important' entities. Some members of the SGs have expressed concerns that the number of institutions obliged to conduct testing may be such that it could cause practical challenges, e.g. with testing capacities, especially given the required frequency of testing. The SGs welcome the suggestion that competent authorities should retain a degree of discretion to assess the appropriateness of TLPT on a case-by-case basis ((Article 2(2) RTS) and to selectively 'opt out' FEs from the requirement.

ESAs response

The ESA welcome the SGs' overall support for the approach on proportionality followed in the draft RTS.

On introducing more proportionality in the TLPT process, the ESAs want to recall that each test will be oranised on a case-by-ase basis and result form a dialog between all parties aiming at performing the most comprehensive, efficient and safe testing exercise.

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.

The SGs agree with the two-layered approach and welcome the approach that membership of a corporate groups should be taken into account in the identification of FEs subject to TLPT. Where ICT systems are shared across different legal entities of the same group, group testing would be preferred. For FEs which belong to a group where the parent undertaking is located outside the EU, and which

operate in the EU with more than one subsidiary or significant branch, the designation of a TLPT authority in one member state as the lead-EU TLPT authority may be warranted.

ESAs response

The ESAs welcome the SGs' overall support for the two-layered approach proposed to identify the financial entities that will be required to perform TLPT in the draft RTS.

The ESAs consider group testing (covered under the concept of 'joint TLPT' in the draft RTS) should not be mandated and that flexibility should be left to FEs and TLPT authorities to organise test at solo or at group level.

Third country entities are not covered in the draft RTS.

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.

The SGs agree, in principle, with the proposed approach, subject to the following observations:

- Some members of the SGs are of the view that the threshold for payment institutions set at EUR 120 billion of total value payment transactions appears low and should perhaps be changed in a way that provides more flexibility for authorities to decide when to include FE in the testing.

- Some members of the SGs are of the view that the criteria for determining insurance and reinsurance undertakings to be in scope of TLPT in Article 2(1)(g) are not sufficient for companies to know whether they are in scope or not. They note that this information is not publicly available, or not available at all (calculations per activity area), so that companies may not be able to calculate objectively whether they would be in scope. They suggest that further clarification may be needed on the criteria, especially specifying the relationships between the clauses (e.g. 10% of total assets, or overall assets in one area).

- Some members of the SGs consider that the envisaged timelines for TLPTs may not be in line with practical experience so far, especially if the inclusion of mandatory 'purple teaming' is kept and suggest that a less prescriptive approach may be warranted.

ESAs response

The ESAs welcome the SGs' overall support for the quantitative criteria and thresholds proposed in Article 2(1) of the draft RTS.

On payment institutions: after discussions with national authorities, the ESAs have increased the threshold to EUR 150 billions.

On insurance and reinsurance undertakings, the ESAs have reviewed the methodology used in the criteria to make it more transparent for market stakeholders.

On timeline, more flexibility has been given in the closure phase.

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

The SGs generally welcome the intended alignment with the TIBER-EU framework and appreciate the limitations inherent in incorporating the original, voluntary framework into a regulatory text. Some members of the SGs note that additional aspects of the TIBER-EU framework may be included in the form of guidance rather than mandatory obligations. These members argue that this approach would better reflect proportionality considerations and a risk-based approach towards testing and avoid undue burden on financial entities.

Annex II 2(a) requires FEs to provide a list of all critical or important function and to explain on which basis a critical or important function is or is not to be included in the scope of the proposed TLPT exercise. In practice, FE usually choose a small subset of critical or important functions for inclusion in the TLPT exercises. Annex II 2(a) would therefore likely require a long list of explanations In the interest of efficiency, the structure of Annex II could be streamlined to focus on the initial list of critical or important functions, the subset of functions included in the TLPT, and the methodology applied in selecting that sample.

It may be beneficial to develop a set of guidelines for additional aspects that go beyond the existing TIBER framework, for example on combined and pooled testing, to provide guidance to FEs on how to apply these new requirements.

ESAs response

The ESAs welcome and take note of the feedback received from the ESA's SGs, and will assess the need to issue complementary guidance in the form of supervisory convergence tools (such as Q&As, guidelines).

On the content of the scope specification document referred to in Annex II: it is important this document provide a broad view of the critical or important functions, which will be narrowed down during the threat intelligence phase.

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.

The SGs broadly agree with the proposed approach. Some members of the SGs are of the view, however, that the mandatory nature of the requirements in Article 5 may present an undue burden on financial institutions and may be counterproductive and detrimental to the successful completion of TLPT. These members recommend including optionality for financial entities when listing requirements in items (a) to (g) of Article 5(2) and suggest that the wording in Article 5(2) should be amended to read: "The control team shall consider taking measures to manage risks…", instead of "The control team shall take measures…".Similarly, these members suggest that item (h) of Article 5(2)

should give optionality to the FE's control team to consider additional restoration procedures with the testers, instead of mandating all the measures listed in the draft RTS. Other members of the SGs observe, however, that divergences in the practical implementation of TLPT testing, especially with regard to risk management measures, could run counter to the legislators' original intent of promoting a consistent methodology and ensuring uniformly high standards of security.

Some members of the SGs believe that FAs should be able to share the risk assessment findings inside their own organisation without being constrained excessively by confidentiality provisions. Other members of the SGs suggest that, instead, the control team should assign relevant roles to help process and distribute findings from the risk-assessment.

Some members of the SGs note that the FE should also be allowed to pause the TLPT in case of a real world attack during the test. Other members note that this scenario should be adequately covered by Article 8(10) of the RTS.

ESAs response

The ESAs welcome and take note of the broad agreement from the ESA's SGs on the approach followed on risk assessment and management in the proposed draft RTS.

As to risk management measures, the ESAs believe those listed are minimum requirements that all FEs should follow.

As to the sharing of information relating to the TLPT, strict restrictions shall apply during the test: within the FE, only the control team members should be in the know (it has been calrified that if needed the composition of the control team can evolve during the TLPT, subject to validation by TLPT authority). However, information on the TLPT can be more widely shared after the test, in particular to maximise the learning dimension of such exercise.

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.

The SGs consider the requirements broadly appropriate. Some members of the SGs are of the view that the mandatory nature of the requirements in Article 5 may present an undue burden on financial institutions and may be counterproductive and detrimental to the successful completion of TLPT (see Q6. above). These members of the SGs suggest amendments, in particular to items (a), (c), (d) and (f) of Article 5, to reflect some optionality for financial entities to have the ability to make exceptions after having performed an internal risk-assessment and listed relevant mitigating factors. They note, for example, that the obligation to request three references for threat intelligence provider (item c) and five references for external testers (item d) from previous assignments may pose challenges. They argue that the nature of such engagements often demands a high-level of confidentiality to preserve the effectiveness of the assessments and that disclosing specific details about prior assignments could compromise the anonymity and security of the clients involved. Other members of the SGs are of the view that the introduction of TLPT as a standard requirement for qualifying FEs will necessarily involve a period of 'capacity-building' to ensure that adequate pools of experienced professional personnel are available.

From a practical point of view, the SGs note that it would be useful to include in the RTS a list of approved certifications for specific roles.

ESAs response

The ESAs welcome and take note of the feedback received from the ESA's SG.

Requirements for testers have been reviewed to address some of the concerns raised through the public consultation, but always keeping in ming the utmost importance of using the most suitable testers to ensure efficiency and safety of TLPTs. In particular, criteria relating to experience has been changed from experience in TLPT to experience in penetration testing and red teaming.

In addition, some flexibility has been introduced through the possibility in exceptional circumstances for FEs to choose TLPT providers that do not fulfil all requirements, subject to establishing an adequate risk management framework for the test and to the agreement of the TLPT authority.

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.

The proposal for threat intelligence providers and external testers to have at least 5 years' experience is aligned with the TIBER-EU framework and could therefore serve as a useful point of departure. Some members of the SGs observe, however, that FEs should be provided with some more optionality, based on internal risk-assessments (see Q7. above).

In the longer run, the SGs suggest that it may be advisable to develop a framework for the accreditation of testers to ensure a minimum standard for providing and conducting relevant services, similar to the approach taken, e.g., by the Bank of England.

ESAs response

The ESA welcome and take note of the feedback received from the ESA's SG.

Flexibility has been introduced for FEs to contract testers that would not fulfil all of the requirements subject to evidencing the exceptional circumstances that in their view justify it and the related risk mitigation measures they have established to address such choice and to the absence of objection from their TLPT authority.

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

The SGs consider the proposed process generally appropriate. The SGs would like to highlight a few areas for improvement as follows:

- Paragraph 42 refers to the TLPT authority to issue an attestation in relation to 'critical systems in scope of testing'. This term does not exist either in the regulation text of DORA, nor anywhere else in the draft RTS and may need further clarification.

- The draft RTS assigns approval and validation tasks to the TLPT authority as part of the TLPT testing process, both ex-ante and for any changes to the TLPT as they occur. The latter may be impractical and the process should allow for greater flexibility, for example by pre-agreeing under what circumstances or scenarios the TLPT authority might only be notified of changes to the 'red team' test plan, without a need for formal approval. A notification procedure instead of an approval procedure may also be more practical in the case of pre-agreed or ad-hoc 'leg-ups'. Similarly, in the event that the testing activities are detected by any staff member of the FE or its ICT TPP, notification of, instead of validation by the TLPT authority may be more practical in order for the testing process to continue without undue delay.

- In general, the proposed timeframes appear appropriate. There may, however, be circumstances where timeframes would need a certain level of flexibility.

- The RTS requires the active red teaming test to be a minimum of 12 weeks. This should be understood as a default but exceptions should be possible, for instance, when a test exercise achieved its testing objectives in a shorter period of time, as demonstrated by the relevant protocols. Based on practical experience with TLPT, some members of the SG are of the opinion that a test period of six weeks (two weeks of active testing per each scenario) is typically sufficient to achieve the objectives of the test and, at the same time, help reduce TLPT test costs for FEs. Other members of the SG note that the TIBER-EU standard recommends a minimum duration of the 'red team' testing cycle of ten to twelve weeks. They note that TLPT should be mirroring a real-life scenario as closely as possible and undue time pressure, by compressing the time available to 'red team' testers, could render the exercise altogether meaningless.

ESAs response

The ESAs have reviewed the timeline in particular of the closure phase, to remove dependencies between the different documents that must be produced during that phase. If necessary in view of specific conditions of a given test, certain arrangements might be agreed between the parties to the test. However the ESAS consider that in order to give testers enough time to mimic real-life conditions, the twelve-week minimum duration for the active red team testing phase cannot be reduced. This is fully in line with the TIBER-EU framework (which next version will reflect this minimum baseline of twelve weeks). It can be increased based on the characteristics or number of parties involved in a test.

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

The requirements for pooled testing lacks detail and present significant practical challenges for FEs, regulators and ICT TPPs. In the absence of guidance under the TIBER-EU framework in relation to pooled testing, it may be advisable to delay the use of pooled testing until such guidance is published. Pooled testing is not common practice across the financial sector yet and significant uncertainty

remains concerning any attempts that have been made by TPPs to run such tests thus far. Once suitable guidelines are available pooled testing could be particularly relevant for FEs within the same group sharing critical business functions provided by an internally shared IT provider.

ESAs response

As this is a possibility given by DORA, the ESAs consider necessary to include more details on the organisation of a pooled tests, both on the side of the FEs (with additional provisiosn on risk assessment and management) and on the side of the TLPT authorities involved in such complex exercise (in terms of cooperation needed).

Similar types of requirements have been added for 'joint TLPTs' for cases where FEs use the same ICT intra-group service provider or belong to a group and use the same ICT systems.

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.

The draft RTS requires several controls related to the use of internal testers. While the SGs agree with the controls listed, some of members consider certain requirements to be too prescriptive and argue that they introduce unnecessary burden and duplication. They suggest, in particular, that items (a.i.) and (a.iii.) of Article 11(1) are usually covered by the job descriptions, and assessed during the recruitment process for internal testers and should therefore be removed.

The SGs note that the draft RTS requires all members of the test team to be employed by the FE or an ICT TPP for the preceding two years. The draf RTS does not currently set out a rationale for this requirement, such as, presumably, the need for internal testers to be familiar with the infrastructure subject to testing. The SGs would welcome a more detailed explanation of that reasoning.

Furthermore, some members of the SG are of the view that some scenarios for 'red team' testing may not need a large team and suggest that a minimum number of two members should be deemed sufficient.

ESAs response

The requirement for a certain duration of past employment by a FE is in view of the ESAs necessary to distinguish internal testers from external ones. To address concerns relating to high turnover in respect of such positions, the minimum duration has been reduced from two years to one year.

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

The draft RTS does not include information concerning the scope of a TLPT should it entail multiple TLPT authorities. There is a risk that the involvement of multiple TLPT authorities could lead to longer and more complicated testing. It would be advisable to incorporate procedural safeguards to ensure that the involvement of multiple TLPT authorities does not result in any material and unwarranted

changes to its scope. The FE should still be allowed to respond to any scope to ensure the test remains rational to their operations across Member States. Most FEs in-scope of DORA TLPT tend to have centralised security teams who operate across all Member States and use the same set of ICT systems and controls. Adding applications on the basis that they are in use in a particular Member State would likely produce little in terms of incremental insights but would most probably result in added complication and difficulty in administering the test.

The draft RTS supports mutual recognition on the basis of three criteria: testing of critical or important functions, use of internal testers, and implementation of the TLPT as a pooled test. The SGs are of the view that these should not be the only criteria to be considered for recognition as there are other, equally important factors for recognition, e.g. whether the TLPT was carried out on common ICT systems and targeting the defensive teams that are involved in the FE's actual operations in the respective Member States. Art. 12(5) may be amended to reflect this criterion. In addition, the report referred to in Article 26(6) and reflected in Annex VII should provide sufficient information to adequately inform a decision on mutual recognition.

ESAs response

It has been clarified that in case a TLPT involves several FEs (pooled TLPT or joint TLPT), for the pooled or joint part of the test, one TLPT authority will be designated as the lead TLPT authority to coordinate other participating TLPT authorities and ultimately make the decisions necessary for the progress of the test, i.e. validation of the scope of the joint or pooled TLPT.

The ESAs confirm that mutual recognition is not granted on the basis of three criteria but based on the attestation which will be delivered if "the test was performed in accordance with the requirements" (Article 26(7) of DORA) i.e. with all the requirements set out under Articles 26 and 27 of DORA, and related Level 2 provisions.

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.

No further comments.

6. Feedback on the public consultation

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
General drafting approach Q1. Do you agree with this cross-sectoral approach? If not, please provide detailed justifications and alternative wording as needed.			
Support for the cross-sectoral approach	- promotes uniformity and simplicity - enables standardisation and harmonisation across the Union - has already proven effective by TIBER-EU - sectoral aspects are already taken into account in various parts of the methodology (threat intelligence and red teaming) - if article 2 on identification of FEs required to perform TLPT is clarified (and appropriately applied - provides flexibility, consistency and cost-effectiveness Bank of England's CBEST Threat Intelligence-Led Assessments has also a cross-sectoral approach	The ESAs welcome these comments.	No change.
Delay application date	will require more adjustments from firms from the insurance sector then from banking sector and for those established in Member States which have not yet implemented TIBER-EU framework ; proposal:	The draft RTS cannot delay the application date set in DORA.	No change.

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
	extension of compliance deadline (PL Chamber of Insurance, Insurance Europe)		
Request to clarify "cross-sectoral"	Does it mean tests should be carried out between different entities within the same sector? (Asso. Espanola de Banca)	The RTS requirements are sector-agnostic ie apply independently from sector to which a FE belongs. Thi is also in line with the approach followed by the TIBER-EU framework.	No change.
Reflection of sector specific aspects in the scoping and scenarios	- Some respondents suggest to reflect sectoral aspects in the scoping phase and the creation of testing scenarios and to pre-describe specific mandatory scenarios. - Sectoral aspects should be more taken into account in the scoping of threat scenarios that are mandatory for testing, as for financial entities not all scenarios are relevant for example payment transactions are mainly for banking institutions. Sectors differ in risk exposure.	Scenarios are already selected based on threat intelligence targeted to the tested FE. There is no obligation that every TLPT has to contain a scenario on a specific topic like transaction payments.	No change.
More sector-specific considerations in the TLPT methodology	- Incorporating mandates in the regulation to conduct tests for assessing the robustness of data protection tools could be particularly beneficial for financial entities,	As per the approach followed by the TIBER-EU framework, the methodology has to be cross-sectoral.	No change.

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
	given the criticality of data security in their operations. - This perspective seeks to understand whether there are provisions within the proposed framework to accommodate such sector-specific considerations, or if there is scope for introducing more tailored approaches within the TLPT methodology to better cater to the unique risk landscape of the financial sector.		
Flexibility	It is important to provide flexibility to meet the specific needs of certain sectors while maintaining the overall cross-sectoral approach.	No specific example provided. Proportionality as guiding principle in its application	No change.
Q2. Do you agree with this approach [on proportionality]? If not, please provide detailed justifications and alternative wording as needed.			
Support for the proposed approach on proportionality	Common set of requirements for all FE makes for an easier compliance with such requirements	The ESAs welcome this comment.	No change.
More proportionality for IORPs	There should be stronger proportionality considerations in Article 2(3) as well as Section II of the RTS in respect of IORPs, considering that:	According to Article 2 of the draft RTS, IORPs are not "by default" subject to TLPT: According to Article 2 of the draft RTS, IORPs can be subject to	No change.

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
	- IORPs pose very low risks to the continuity of core financial services such as IORPs are not within the scope of the DORA TLPT set-up - pension policy is a national competence and the IORP II Directive prescribes minimum harmonization, IORPs vary widely between Member States. That makes it hard to specify EU criteria for IOPRs on the application of TLPT. National TLPT authorities seem better placed to determine whether IORPs and their service providers have to perform TLPT	TLPT only if they are opted in by their competent authority.	
Proportionality should also apply at the level of requirements	Proportionality should be applied at the level of the requirements associated with the testing process reflecting the varying size/profile and ICT resources of financial entities that may be required to complete TLPT under DORA. There should be a possibility to opt-out or adapt certain requirements in respect of selected FEs: - number of participants to the TLPT and the requirements related to the establishment of organizational and procedural measures; need to distinguish between the control	TLPT as described in DORA in its essence an advanced testing method, therefore it does not make sense to make 'TLPT-light'. Less advanced testing is covered by Article 24 of DORA. Requirement that TLPT shall be carried out on live production systems is already embedded in Articles 3(17) and 26(2) of DORA.	No change.

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
	team, control team lead, blue team, and purple team may not be feasible for smaller sized organizations who may not have the personnel and organizational structure to cover so many different and independent teams and functions; arrangements relating to the secrecy of the TLPT should only be mandatory where possible. - 12-month minimum duration of the red team testing phase - Need to carry out the test on live production systems		
Application of proportionality in the selection process should be revised	- The operational structure of ICT systems for FEs operating in several MS (using same ICT systems with central control and internal testing programs) as well as TLPTs already carried out should be considered for the identification and in the implementation of the requirements. - systemic importance is the most important metric to ascertain whether a financial entity should undergo TLPTs. As currently formulated, Article 2(3)(a) doesn't appear to specifically address the issue of whether a financial entity actually presents a	DORA sets out the general requirement for authorities to identify FE in scope of TLPT, while the RTS further substantiates the requirements (as required by article 27(11)(a) of DORA). Once identified by TLPT authorities under Article 2(3) FEs should be informed as soon as possible before the actual request to start a test is notified by the TLPT authority. Although only TLPTs carried outin accordance with DORA will be eligible for an attestation under DORA, the fact that a FE has already undergone a TLPT should be taken into account by the	No change. Clarifications on the consideration given to the operational structures of FEs in Articles 2(3), (4(a)(vi) and 4(b)(ix).

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
	systemic risk to a financial market, either at the Union or nation state level. - The proportionality principle within the RTS applies to microenterprises only, leaving a vast number of FEs in-scope of TLPTs under DORA. This will constitute a significant undertaking for a large number of smaller FEs alongside significant oversight of TLPT authorities (with a minimum of two employees in the TLPT authority supporting each test). Paragraph 11 allows greater flexibility for authorities to set the frequency of testing, and we believe this should be emphasised further to allow for the feasibility of the RTS being administered. Opting out branches of larger FEs, in favour of a focus on the most significant EU entity of the group is seen as a practical way to reduce the number of firms in scope and make the frequency proposed in the Level 1 text more achievable.	authoritiesi in their assessment of the ICT maturity of a firm. Microenterprises are out of scope TLPT, as other FEs referred to in Article 16(1) of DORA (Article 26(1) of DORA).	
RTS should encourage	in order to benefit optimally from TLPT a certain maturity is required: entities that are not mature	DORA Article 6(1) generally requires the ICT risk management framework to be documented and	No change.

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
improving digital operational resilience	enough for TLPT be required to give a path toward a sufficient level of ICT maturity in order to undergo TLPT. The wording of point 23 implies that systemically important organisations with low ICT maturity may not need to undergo testing. Low maturity should not be an excuse for an entity not to perform these activities. Systemically important entities should be tested regardless of maturity, and it is particularly important to identify systemically important firms that have a low level of cyber maturity compared to their peers. Regarding the risk assessment to be conducted by TLPT authorities, Article 2(3)(b)(h) refers to the maturity of [a FE's] operational ICT security detection and mitigation measures. This could create a disincentive for smaller firms to develop their capabilities, and could negatively impact those firms with more advanced approaches. We would propose amending this to refer to the complexity of such measures rather than the maturity. RTS should encourage less mature FEs to improve their DOR and global DORA at EU level.	reviewed and improved – so it seems redundant to require for the same in TLPT RTS.	

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
Alignment on NIS 1 and 2	This should be in line with the criteria set out in NIS 1.0 and NIS 2.0 national implementation in terms of the proportionality aspect. Proportionality should be in line with NIS 1 and NIS2 national implementations	As specialised legislation aiming specifically at the financial sector DORA supersedes NIS 1 and NIS 2	No change
Criteria to select entities required to perform TLPT 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.			
Qualitative criteria are too vague and subjective	- The two-layered approach is not clear enough or too open to be understood by financial entities and may lead to a wider scope as intended and so left too much to the discretion of the TLPT authorities, that can have divergent interpretations - Additional guidance and/or clear scales and thresholds to include in the RTS for each criterion is needed to ensure a consistent and repeatable assessment process across the EU Member States	The ESAs see the two-layered approach as on the one hand, ensuring that at least the most relevant financial entities are subject to TLPT across all Member States under Article 2(1); and on the other hand, allowing TLPT authorities to opt in financial entities in their remit which they deem suitable to perfom TLPT, based on a case-by-case assessment of their impact, systemic character and ICT risk profile and taking into account the proportionality principle. The qualitative criteria are meant to bring some flexibility in the selection process and along the years.	Clarification in Article 2(3) of the draft RTS

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
	- need for clarity regarding the criteria and process employed by the regulator to determine their selection - The qualitative criteria could capture FE that do not represent major financial stability concerns such as IORPs - to enhance security maturity for the whole industry it would be better to have same requirements for all entities that should be able to adjust requirements according to their risk exposure (ICT maturity, geopolitical risks, etc.) - The ESAs should develop, for each qualitative criteria, scales and thresholds to be included in the RTS - The criteria "risk profile, "threat landscape" and "complexity of ICT architecture" (art2(3)(b)a, b and d) are : o overly broad and very difficult to practically assess on a regular basis. Their assessment depend on the threshold used to determine	Qualitative criteria shall be assess cumulatively to allow selecting only the most relevant financial entities to perform TLPT.	

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
	the level of risk that make a FE ICT mature o regularly evolving leading a FE to be eligible to TLPT one year and maybe not the following		
Some qualitative criteria are not appropriate	ICT contractual arrangement should not be taken into account in the decision to require TLPTs on a FE and ask for the deletion of criteria c, d, e of Article 2(3)(b) of the RTS	Points c, d and e do not refer to contractual arrangements	No change.
Clarify if criteria to identify FE shall be used in combination or alternatively	It is not clear if a criterion can be used independently by a TLPT to identify a FE or if a combination of several criteria is necessary and are in favour of the second option -	Criteria shall be assessed in combination i.e. cumulatively, and not alternatively.	Article 2(3) has been clarified to provide that the TLPT shall assess whether FEs other than those referred to in 2(1) shall be required to perform TLPT taking into account their impact, systemic character and ICT risk profile, assessed on the basis of all of the [qualitative] criteria".
Need to specify a hierarchy between the qualitative criteria	- Current draft RTS does not provide any priority/hierarchy to the given criteria and sub-criteria. It is not clearly established whether a FE is required to perform TLPT as soon as it meets at least one of the criteria, more than one, or all of them. Define size	The ESAs consider there is no hierarchy between the criteria: all criteria including systemic importance, but also impact and ICT maturity, shall be assessed by the TLPT authorities in combination.	Clarification in Article 2(3) that all criteria shall be assessed.

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
	criteria detailed in Article 2, paragraph 3, section (a) based on number of employees - Only entities that present systemic risk to the financial sector at a Union or national state level should be eligible for TLPT - Criteria of "systemic importance" should only cover truly systemic entity ie. where incidents and interrruptions affect the financial system as a whole or other societal systems - "systemic importance" should be considered more important than "ICT maturity". FE of systemic importance should be required to conduct TLPTs even if not in scope of Article 2(1). - The criteria in article 2(3)(a, b, c) could be categorized as low/medium/high and that a FE can be identified in case it meets high criteria		
Clarify ICT maturity assessment	The TLPT authority must also sufficiently take into account (as part of the maturity test, or in addition to it) the organization's IT capacity, so that the impact of a TLPT on daily operations is limited.	Assessment of ICT maturity of a FE is an important element of the selection process of FEs required to perform TLPTs. It is also important that (in accordance with recital 56 of DORA and recital 4	No change.

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
	Moreover, this criterion will become less and less relevant as DORA will require a common level of cyber resilience. Firms should be potentially subject to TLPTs even if they are not mature enough The concept of maturity needs to be defined in some manner to give a better understanding of what "mature enough" represents; need to clarify how and by whom maturity assessment is made. Proposals: - if all TLPT requirements can be realised with enough expertise to preserve FE continuity as regards the modalities of the TLPT (eg. live production test) - How digitalized the FE is in terms of business functions and customer services offerings that have a critical dependency on ICT services, or -	of the RTS) that the organization is sufficiently mature to be able to carry out a TLPT. Suggestion could be to elaborate the relevant recital to describing the requirement in relation to the actual ability to perform TLPT, including having the necessary ressources, one relevant element in the assessment being if the FE has performed TLPT before, however without describing it too specific, thus not allowing for the FEs to adapt their business to avoid TLPT.	
Clarification for investment funds and asset managers	- Clarify whether investment funds would fall under the scope of this activity (e.g. when belonging to a banking group or as separate entities)	Investment funds are not mentioned among the categories of financial entities listed Article 2(1): therefore they are not "by default" identified as FEs required to perform TLPTs. Their submission	No change.

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
	- asset managers (including Investment Fund Companies) should not be subject to TLPT tests, based on recitals 4 and 56 of DORA	to the requirement to perform TLPT can only result from a case-by-case assessment by their TLPT authority under Article 2(2) and (3). The fact that they would belong to a G-SII or O-SII does not trigger their submission to the requirement to perform a TLPT (this is for credit institutions identification only).	
Exclusion of Credit rating agencies	Credit rating agencies should be excluded from the application of the TLPT RTS due to the proportionality principle and lack of complexity in CRA business models relative to other financial sectors and the resulting limited scope of such testing.	The mandate in Article 26(11)(a) of DORA to define criteria for TLPT authorities to assess which financial entitie shall be required to perfrom a TLPT does not allow to exclude financial entities from the scope of TLPT. Credit rating agencies not being listed among those types of financial entities mentioned in paragraph 1 of Article 2 of the draft RTS, their submission to the requirement to perform TLPT can only result from a case-by-case assessment by their competent authority (ESMA).	No change.
Exclusion of IORPs	IORPs should not be required to perform TLPT due to: - their overall risk profile, nature, scale and complexity of its servces, its activities and operations.	According to Article 2 of the draft RTS, IORPs are not "by default" subject to TLPT: they will be required to perform TLPT only if they are opted in by their competent authority.	No change.

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
	- IORPs do not work with real time data and are in this sense less prone to cyber threats or negative consequences due to service interruptions, compared to other financial players.		
Participation of ICT TPP in TLPTs	A bigger concern relates to the fact that certain ICT third-party service providers will be required by their financial entity customers, per Article 30(3)(d) of the Regulation, to participate and cooperate in those financial entities' TLPT. For those ICT third-party service providers, it is impossible to anticipate how many financial entity customers will require such participation and cooperation and therefore difficult to prepare operationally in terms of staffing and scaling. Given the number of Member States and financial entities involved, there is a significant risk of a single ICT third-party service being overrun with TLPT exercises, which would impose an unreasonable administrative and financial burden on them and result in an increase in the cost of services. Therefore, there should be a mechanism in the regulation to avoid this. For example, relevant ICT third-party service providers should be entitled to participate in the	Cooperation between authorities is designed to organise the most comprehensive but also feasible TLPTs. TLPT authorities should assess, based on communication with financial entities in their remit and, as the case may be, their ICT service provider, what is the most suitable size and timing for each test.	Requirements in terms of supervisory cooperation have been clarified (Article 14), in particular in cases where the TLPT is envisaged as possibly involving several FEs and/or an ICT service provider (pooled or joint TLPT). The TLPT authority will in fine validate the scope and size of the TLPT, to ensure its effectiveness and safety.

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
	Control Team and Blue Team and to be involved in determining a TLPT's scope and timeline so that resourcing can be better managed		
Considering operational structure of ICT systems	We note that the ESAs have not considered the operational structure of ICT systems for financial entities who operate across multiple Member States. In the majority of cases, mature financial institutions with multiple entities and branches will utilise the same ICT systems with central control and cybersecurity departments that administer their internal testing programs. The argument used for the proportionality principle within the RTS does not relate to the operational practices of financial entities operating in the EU and we recommend that consideration of the structure of the specific financial entity, alongside prior TLPT tests across other TLPT authorities, should be included within any identification.	The identification of FEs required to perform TLPTs is carried out by TLPT authorities at legal entity level but can take into account the belonging to a group using the same ICT intragroup services provider or th same ICT systems (authorities can select the most relevant FE to be tested to avoid multiplying tests on the same systems). In addition, joint TLPTs can be organised to test in common several identified FEs using the same ICT intra-group service provider, or belonging to the same group and using common ICT systems.	Clarification of the consideration of group belonging in the identification of the FEs that will be required to perform TLPTs and of the concept of 'joint TLPT' and related TLPT process..
Disclosure and right of objection to identification	The TLPT authority should disclose the rationale in opt a financial entity in and the financial entity should have the right to object.	The identification as FE required to perform a TLPT is an administrative act, the usual possibilities of objection and appeal exist.	No change
A more collaborative	- It is essential that the FE provides TLPT with information regarding the potential overlap	Information on systems supporting critical or important functions will be provided by the FE to	No change.

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
approach between FE and TLPT authority could be necessary	of ICT systems and controls within their groups. - It may be more efficient that the FE themselves assess the article 2(2)(b) ICT risk related factors and submit some summarized level of information to the TLPT.	the TLPT authority through the scope specification document.	
Clarify process for TLPT authority to communicate decision on requirement to perfom TLPT	- The FE identified through the qualitative criteria should have a period of at least 9 months to submit the initiation documents to the TLPTa and should not be required to fulfil any requirements prior to the notification from the TLPTa. - It is not clear if the selection of a FE implies a one-time TLPT or adherence to recurring tests indefinitely, nor if the obligation to conduct TLPT is every 3 years from the closure of the preceding TLPT exercise or every 3 calendar years. - RTS should state that the TLPT authority should inform all FEs, both those obligated to conduct TLPT and those exempted from the requirement	The deadline to submit initiation documents only starts from the communication by the TLPT authority of a notification under Article 6(1) of the draft RTS. Such notification is not the one through which the TLPT authority informs a FE that it is subject to TLPT (which should in principle be made earlier). Article 26(1) of DORA clearly establishes a recurring obligation to to carry out TLPT "at least every three years" for the financial entities identified as in scope of the obligation. The ESAs had no mandate on the way TLPT authoritis should communicate their decision to include a FE in scope of TLPT or not. These procedures shall be set out at national level.	No change.

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
	- Further clarify the process related to the regulator's communication procedures, lead times before the TLPT takes place, and outlining expectations for the frequency of testing (one time vs recurring tests)		
Consideration for groups of FEs	- It is not clear how TLPT authority(ies) of the Member State(s) will coordinate inclusion of group entities operating in different countries into scope of TLPT - It is necessary to clarify that Article 2(2) applies also to FE selected through Article 2(3) criteria - Article 2(2) (second sentence) only includes FEs belonging to the same group on the basis of the criteria in paragraph 1(a) to (g). This excludes groups which consist of IORPs and/or IORPs and insurance undertakings since IORPs are assessed of the criteria listed in Article 2(3). The paragraph should be revised to cover any FE. Where more than one FE belonging to the same group meets the criteria set out in points (a) to (g) of paragraph 1 or paragraph 3.	As to the selection of FEs belonging to groups, Article 2(3) already includes the possibility for TLPT authorities to take into account (point (a)(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" and point (b)(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". As to the conduct of joint tests, clarifications have been made in the RTS, in particular on the cooperation with other TLPT authorities.	Clarifications have been brought to the provisions relating to cooperation of TLPT authorities in case of joint test (over several FEs using the same intragroup ICT service provider of common ICT systems) (Article 14)

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
Groups of FEs with parent company based in non-EU country	How to handle the situation if the group parent or group internal ICT service provider is located outside the Union? Article 2(2) additionally assumes that the parent undertaking of a group of financial entities is based within the EU. This fails to accommodate those entities where the subsidiaries are within the EU (with different lead overseers) and require clarification.	DORA scope is limited to financial entities established in the EU and the ESAs have no mandate concerning third-country entities.	No change.
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.			
No automatic selection	Article 2 (1): "TLPT authorities shall consider requiring all of the following financial entities to perform TLPT …" instead of " TLPT authorities shall require…"	The ESAs consider the types of FEs listed under Article 2(1) shall by default be required to perform TLPT as they are considered satisfying all the criteria listed in Article 26(8), third subparagraph.	No change.
Criteria regarding credit institutions	The term "systemically important institutions" must be defined and only systemically important financial institutions (SIFIs) should be addressed under the RTS on TLPT	The concepts of "global systemically important institutions (G-SIIs)" is defined by reference to in accordance with Article 131 of Directive 2013/36/EU of the European Parliament and of the Council, the ESAs consider there is no need to define it in the RTS.	No change.

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
Criteria regarding insurance undertakings	- Lacks transparency: entities and their ICT TPP cannot determine if they are identified or not (only authorities can make the relevant calculations) - Is not in accordance with the pan-European character of DORA as its paragraphs (ii) and (iii) lays on national characteristics, nor with the proportionality principle as an insurance in a small Member State could be required to perform TLPT while an equivalent insurance in a bigger Member State would not - Provisions that allow for a designated FE to immediately inform any of its ICT third-party providers likely to be involved in its TLPTs of this designation could be added. - Paragraphs (ii) and (iii) do not specify to which financial year the GWP and total assets should correspond so it is necessary to explicite that they both refer to the last available financial year - It is not clear in paragraph (i) whether an undertaking needs to have GWP above the	The ESAs have reviewed the criteria applying to insurance and reinsurance undertakings to include a more transparent calcaultion method.	Modification of Article 2(1)(g)

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
	average of the MS for all or at least one of the activities related to life, non-life, health and reinsurance - Covers the (ii) criterion oly the previous financial year or each of the previous two financial years as in criterion (i) - Combination of average and 10th percentile unclear; whether it is valid for all criteria or not - It is necessary to clarify that the (ii) is fulfilled in case GWP are above the 90th percentile of the GWP distribution - Whether the entity is defined as systemically critical or from a financial stability perspective is not precised: current risk of over-designation - 500 million € GWP appears to be way too low (for the market overall). Given the cost impact is estimated around 500k€ average (with 10 to 12 weeks of testing) this is not proportionate to risk; it should be increased to EUR 1.000 million.		

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
	- Reinsurance and non-life insurance shall not be included in the quantitative criteria		
Criteria regarding payment institutions	- when interpreting Article (5)(5) of Payments Services Directive (EU) 2015/2366, it is not clear whether the sum of incoming and outgoing payments or only one of the two is to be considered here. It is also questionable whether securities trading is included. - The figure of EUR 120 billion of total value payment transaction is too low and will result in too many institutions covered	The ESAs have reviewed the criteria to increase the threshold to EUR 150 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.	Modification of Article 2(1) (c)
Criteria regarding trading venues	- The measurement of market share at the national level should be with reference to market participants in that MS rather than turnover - The venue with the highest share for a given MS could be located anywhere in the Union - Identifying the largest turnover venue in each MS will lead to disproportionate outcomes in terms of including potentially very small domestic venues in scope	The ESAs have considered the comments made and the outcome of the assessment made on this basis and decide to keep the same criteria, and will assess the need for additional supervisory convergence measures in the future..	No change.

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
	- Whether the relevant amount refers to the sum of incoming and outgoing payments or only one of them is to be considered. It is also questionable whether securities trading is included - Proposed criteria for trading venues do not reflect the systemic character enough. A more suitable criterion could be one that does not distinguish between different financial instrument classes but considers the highest market share of a venue across all asset classes. - criteria at national level are too broad and may cover too many entities. In national market with a high competition (like in GER) a trading venue might have a market share of 35% in an specific financial instrument and may be identified to perform TLPT. - Not every asset class has a systemic character by nature: the RTS should not distinguish between different financial instruments but consider the highest market share of a venue across all asset classes PLUS absolute values. In case that		

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
	there is only one national trading venues or only Article 2(f)(ii) should be applicable.		
TLPT process Q5: Do you consider that the RTS should include additional aspects of the TIBER process? If so, please provide suggestions.			
Scoping	Several entities raised concerns about the scoping in the IT security law. One entity wants to maintain influence over the scope and critiques the Level 1 text. Another noted that Annex 2 lacks a requirement to indicate if a Critical or Important Function (CIF) was previously tested, important for consecutive tests. An institution emphasized that more CIFs in scope don't necessarily mean better tests and pointed out potential repetition in Annex II, 2a..	Many of these concerns raised relate to the Level 1 and as such are out of the mandate of this RTS. It is correct that knowing which Critical or Important Functions had been tested befor may be relevant for consecutive tests.	Modification of Annex VIII, details of attestation of TLPT.
Technical testing methodology	The RTS leaves the scope of the required TLPT methods open to interpretation. TIBER-EU advocates, in a non-prescriptive way, testing methodologies based on weaponization, reconnaissance, delivery, exploitation, control and movement, and actions on target. Although TIBER-EU makes it clear that these areas are purely an example of testing methodologies that can be deployed, it would be beneficial for the RTS at least	The RTS only contains the legal requirements a TLPT has to fulfil. If concrete testing methodologies were required, this would reduce the flexibility required for TLPT. For examples and best practices, the TIBER-EU Framework remains available.	No change

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
	an indicative testing methodology of this kind, given the numerous different stakeholders (threat intelligence provider, control team and testers) that are involved in determining the correct testing methodology for the relevant FE's TLPT.		
ICT TPP involvement	- The proposed RTS should also make provision for the involvement of an ICT third-party service provider throughout the entire testing process, where that provider is supporting the FE's critical or important functions. Its clear from the definition of "control team" within the RTS, that some relevant staff from an ICT third-party service providers will inevitably be involved in at TLPT, but the RTS does not expressly state where ICT third-party service provider participation is particularly relevant or important for a TLPT. As such, the RTS should expressly permit the involvement of ICT third-party service providers in the TLPT process, whenever relevant. - It should be made clear that the ICT TPP is not included in the control team by default, but only when relevant. This should be done in order to	The RTS has been clarified to allow the FE to include in its control team staff of its ICT TPP if this is considered relevant in consideration of the scope of the TLPT. The initial composition of the control team and any subsequent changes shall be validated with the TLPT authority.	Changes in Articles 1(1) and 8(4).

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
	not provide sensitive information to the ICT TPP unnecessary. - More clarity on expected 3rd party involvement in TLPT and the scope of such assessments extending beyond the FE. Usefulness of using 3rd parties in testing is questionable as other tools may be better for assurance purposes. Coordination may be very hard.		
No additional TIBER element necessary	No additional elements should be added, because of the cost-benefit ratio. Align only with DORA.	No need for change was identified	No change
Cross jurisdiction testing	Cross jurisdiction testing like with CBEST, BoE, should be clarified.	This is out of the ESAs mandate. This RTS requires TLPTs to be carried out in accordance with its requirements.	No change.
Elements of TIBER to be changed	TI providers may be internal or workshops or collaboratively sourced for smaller entities Scoping meeting and TI/RT handover should be mandated No mention of collaboration of internal and external TI providers Timeframe of 12 RT weeks is too much	While TI providers cannot be internal (the outside perspective is always needed) nothing in DORA or this RTS prevents a cooperation between internal and external TI experts. The 12 week red team requirement is in alignment with the updated TIBER framework.	No change

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
	TI and RT phases need to be better defined in case of weeks and team composition. Multiple parties approve testing conclusion that may introduce COI. - Annexes 1,2 may be confusing.	No individual meetings have been mandated to allow for maximum flexibility.	
TLPT authority involvement	Conflict in RTS recital 13 with L1 26 (2) on the scope and the influence of TLPT authority on it. No expectations beforehand. Scope should be limited to ensure safe and efficient testing. Not all CIFs should be in scope and scope should be balanced. Recital 5a can be redrafted to include ensure adequate and safe testing. Inadequate guidance on multiple TLPT authority involvement, clarifications needed – More authorities should not mean increase in scope. Recital 21 indicates that test managers may influence the results of the testing and this should be removed.	No requirement in DORA to test all CIFs (Article 26(2) of DORA). The involvement of the test managers has been aligned with the involvements of the test managers in TIBER-EU.	No change.
Purple Team	It should be an optional element of DORA TLPT.	The ESAs have decided to make purple teaming a mandatory element of the TLPTs to be carried out under DORA. If no limited purple teaming exercise is used in exceptional cases during the red team	No change

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
	There should be more guidance on how to do Purple Team in DORA TLPT (scope, duration, methodology, potentially duplicate effort).	testing phase, a purple teaming exercise shall be carried out the closure phase. The TIBER-EU framework should be revised shortly to include such change.	
Remediation plan	- There should be guidance on how to verify and follow-up the remediation plan.	This is not part of the TLPT process and is for the supervisory authority to carry out.	No change.
Alignment with TIBER terminology, deliverables and meetings	- Divergence in terminology between TIBER-EU and the RTS could lead to misunderstandings. For instance, we should harmonize "WT" and "CT", "External Testers" and "RT". - Establish minimum standards for meetings, clarifying the roles and responsibilities of the stakeholders. In general, include an exhaustive list of required deliverables, meetings and participants in a TLPT. As in TIBER, all phases should have a timeline defined (which is not the case for TI, Purple Team & TCT validations).	A RTS cannot precisely replicate TIBER-EU framework. For example, DORA terminology has to take precedence over TIBER terminology. A recital clarifies the correspondence between the TIBER terminology and the DORA one. Encouragements to hold meetings at certain stages of the process is also embedded in a recital. Recital 15 already encourages parties to organise meetings for the main steps of the TLPT process.	No change.
Generic threat landscape report	- The TIBER Generic Threat Landscape report could be a construct that would benefit the participants to share cost and an aligned view on the generic threat landscape	This is not a key step of the TIBER-EU framework amd the ESAs did ont consider it essential to include in the DORA TLPT process. Nothing however prevents from preparing one.	No change.

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
Guidance to include ICT TPP	- The risks of including an ICT third party service provider in the TLPT should be better articulated. - When an ICT Service provider is part of the CT, the management of the ICT TPP should also be responsible for scope validation. An amendment is suggested for Article 6(4). - There should be more guidance around how to include an ICT TPP in the TLPT in general (scope, role & responsibilities). The RTS should require (i.e. make mandatory) the collaboration with Cloud service providers but there is scepticism over the added value of such collaboration when the scope only covers functions of a financial entity (customer of the cloud service provider).	Article 30(3)(d) of DORA already requires contractual arrangeemnts on the use of ICT services supporting critical or important functions to include the obligation of the ICT TPP to participate and fully cooperate in the financial entity's TLPT.	Clarification that the participation of a staff member from the ICT TPP in the control team should be proposed by the financial entity and validated by the TLPT authority.
Threat Intelligence	Additional threat intelligence sources should be possible during the TI phase. Not only external threat intelligence provider, but also threat modelling, internal TI providers, sources and assessments.	External threat intelligence providers should always be used. However, nothing in DORA or in this RTS prevents from using additional TI ressources. Nothing limits sources for threat intelligence.	No change.
Control Team Composition	What are the rules to establish a control team in DORA TLPT? Is it fully at the discretion of the FE?	The ESAs have clarified that the initial composition of the control team which shall be proposed by the FE before submitting the scope specification	Change in Article 8(4) to introduce TLPT authority's validation right in respect of the

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
		document, and that any further change to this team, shall be validated by the TLPT authority.	initial composition of the CT, and of any further change.
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.			
TLPT should be conducted in a test environment	Certain risks must be considered, leading to adjustments in approach or implementation, particularly in production environments. If a financial entity (FE) delegates IT to a group entity, the TLPT conducted on a production environment could impact all entities within the Group. This could conflict with local regulations that prohibit TLPT on production environments.	This cannot be changed as DORA requires TLPT to be conducted on live production systems (Articles 3(17) and 26(2)).	No change.
Clarify responsibility for risk assessment / management	- The impression is that no risk assessment process is mentioned for the standard TLPT, which means, there is no clarity on who will endorse the risk management and assess risks and who takes responsibility. **If third parties are involved or tests are conducted jointly**, it is unclear how to manage the risk in the context of an intra-group arrangements. As an option: to use the same the TLPT service provider for several entities belonging to the same group	Article 26(5) of DORA: "Financial entities shall, with the cooperation of ICT third-party service providers and other parties involved, including the testers but excluding the competent authorities, apply effective risk management controls to mitigate the risks of any potential 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."	Clarifications of the responsibilities of FEs involved in a TLPT involving several financial entities (Joint or pooled TLPT) (Article 6)

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
	- There are no specific risk management requirements for tests with ICT service providers and/or for pooled tests. The independence of the risk management of an ICT third-party service provider in multi-client operations is not given sufficient consideration. (Finanz Informatik GmbH) **The ICT TPP should be responsible for risks that the test has a negative impact on other customers or internal processes of the service provider**. The financial institution's control team can only assess and manage the risks for its own organization. - If the **tester is external**, part of the risk management responsibility shall also be in its hands (e.g. to avoid causing excessive damages in the TLPT process) - **ICT Third-Party providers** should be responsible for managing possible negative effects of the test towards other customers. FE's control teams can only manage the FE's risk as they have no sufficient insight, influence nor mandate to manage that of other customers and/or suppliers.	Based on the above, the ESAs have clarified that even in case of a TLPT involving several FEs (joint or pooled test) each FE shall carry out its own risk assessment and establish its own risk management measures. It has also been clarified that the risk management of the joint or pooled aspects of the test shall be carried out by the control team of the designated financial entity.	

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
Risk identification	- Risk management is an extremely broad discipline - it would be useful if this information could focus on the types or categories of risks to be considered, i.e. "focus on risks related to operational impact, loss of information or integrity, threats to confidentiality or availability of critical and important functions" - FEs should be under a specific obligation via the RTS to consider the potential impacts or risks of their proposed TLPT on third parties (including, where relevant, third-party ICT service providers and their customers falling outside the scope of the Level 1 text)	A list of types of risks to be considered is already provided in Article 12(3) of the RTS.	No change.
Risk assessment	- Clarify acceptable risk to be identified and consequences for FE if identified risk cannot be accepted - It would be helpful to have more detail on the scope/methodology used for the risk assessment that must be performed prior to the TLPT. - The top management must approve the potential risks that stem from conducting TLPTs	Possibility to share risk assessment within the FE: Article 4(2)(a) already limits access to information pertaining to any planned or on-going TLPT on a need-to-know basis to the CT, management body, testers, TIP and TLPT authority. The possibility for TLPT authority to challenge FE's risk assessment already exists: Article 8(9) of the draft RTS requires the control team to consult the TLPT authority on its risk assessment and risk management measures and the authority can ask	No change.

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
	- Before the test: risk assessment to be shared within the FE on a need-to-know basis; after ccl of TLPT: to be shared broadly thoughout the FE - Clarify that FE must be willing to accept some level of risk due to inherent risk in TLPT: TLPT authority should have some mechanism to challenge an overly adverse risk assessment conducted by a FE. Article 6(7) of draft RTS addresses the other extreme (Norges Bank)	them to review them to them "should they not adequately address the risks of the TLPT"	
Risk management	- Risk analysis should be performed prior to intiating a TLPT and that the findings should be clearly documented in an engagement letter which would serve as an agreement (outlining the scope of the tests, the roles and responsibilities of the red team, the relevant authorities, and any TPP involved) in order to ensure that all parties have a mutual understanding of the testing parameters, the associated risks and corresponding mitigation processes. - To ensure consistent application in the EU of this approach, we would appreciate further	- Although engagement letters such as thos described in the comment are not mandated under the RTS, nothing prevents the parties from agreeing on such aspects of the TLPT. - Further guidance on type of risk management expected: not further detailed under TIBER-EU - The TLPT is managed by the FE on its own systems. Hence the FE has to do the risk assessment and not the providers or the TCT. - Possibility for FE to challenge TLPT scenarios: not relevant. TLPT scenarios not proposed by	No change.

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
	guidance on what type of risk management is expected of the financial entity for the specific TLPT risk. - When considering potential impacts on the financial sector as well as on financial stability at Union or national level (as stated in Article 5(1)), risk assessment and risk management should also be the responsibility of the TCT as defined in Article 1(6) and the threat intelligence and test providers. - Important that the FE's risk management is given the opportunity to challenge the TLPT scenarios. A TPLT authority may significantly increase the risk of a TLPT by proposing test scenarios that are broad or vague, or that do not relate to the real-world operation of an institution's ICT systems. This approach assumes continuous cooperation between financial institution and TLPT authority during the testing so it may not be feasible from the operational perspective.	TLPT authority but by TIP and testers, selected by the FE's CT and approved by TLPT authority. - Continuous cooperation between the FE and the TLPT authority during testing: this should effectively be the case, with continuous exchanges between the FE's CT and the TLPT authority TCT (as TCT has to approve most decisions made by CT).	
Risk management requirements for	- We believe that when third-party ICT providers are being brought in scope of a TLTP they should	Article 1 of draft RTS has been clarified to provides that control team of the FE can include, where relevant in consideration of the scope of the TLPT, staff of its ICT TPP (and the CT is	Change in Article 1

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
TPPs or Pooled tests	be invited into the risk assessment process where it pertains to their services. - Our concern is that in the context where the TLPT concerns SaaS services, the Control Team will not be able to assess appropriately the risks of carrying out TLPT in respect of software that is delivered as SaaS service by an ICT third-party service provider (due to the impact on other tenants in a multi-tenant environment) unless the service provider is involved in the Control Team risk assessment. Therefore, we strongly suggest that SaaS service providers be entitled to be part of the Control Team. - The third-party should always have the right to representation on the control team and participation in other phases of preparation, execution, and closure of the TLPT as it relates to the third-party. - we would propose that references to staff of TPPs being members of the blue team and the control team should be removed to allow for greater flexibility in firms' implementation.	responsible for conducting risk assessment/management).	

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
	It is imperative that a cloud services provider receives prior notice and adequate information about the nature and content of a TLPT before it takes place. We suggest integrating changes to ensure that ICT third-party service providers are involved in the definition of appropriate processes and communication channels, as well as the rules of engagement of any TLPT that involves their services.		
Possibility to hire consultants to carry out risk assessment and management	- Allow financial entity to be accompanied by an external provider/trusted partner during their risk assessment (the risk assessment still need to be validated by internal decision makers) Introduce the possibility for smaller FEs lacking the appropriate resources and meeting certain thresholds to hire an experienced consultant to perform assess risks for them.	This is not prevented in DORA or RTS but the ESAs expect the risk assessment and risk management process is caried out by the financial entity itself.	No change.
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.			
Support the current RTS	A number of respondents expressed their support for the existing criteria.	No change necessary	No change

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
No mandate	Article 26 of DORA does not give the ESAs a mandate to detail the criteria set in level 1 for external testers	Criteria to select testers and TIP are risk management measures which are part of the specific TLPT testing approach (Article 11(c) of DORA).	No change.
Criteria are too strict, market restriction	The feedback on Article 5.2.d raises concerns about high entry barriers for external testers, potentially leading to market shortages and increased costs. Some respondents argue that the requirements could cause competitive distortions, especially disadvantaging testers from regions where TIBER-XX is less established, and call for more flexibility to allow financial entities to select from a broader pool of testers. Some suggest phasing in TLPT implementation and allowing delays if safety concerns arise. Others recommend reducing or suspending requirements during the DORA introduction to prevent cost hikes and poor cost-benefit ratios. There are calls to define requirements as recommendations, reduce the 5-year experience requirement, and assess suitability through comprehensive presentations. Concerns include potential shortages of providers, increased dependency on a few providers, market entry barriers, and higher costs. Market research to ensure provider availability and adjusting criteria to focus on	It is acknowledged that the market for testers and threat intelligence providers is currently still developing and that in exceptional circumstances it may not be possible to find providers who fulfil all criteria. However it remains of the utmost importance that providers are of the highest quality due to the sensitive nature of TLPT. As a result the requirements have only been slightly lowered (from experience in threat intelligen led red team testing to experience in red teaming and penetration testing). Further a possiblitly was introduced to hire providers how do not fulfil the requirements, provided that the FE accepts and mitigates the additional risk this introduces.	Changes to Article 5

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
	individual tester experience rather than company history are also suggested.		
List of certification / centralised certification	Several entities provided feedback on certification standards for testers. They suggest replacing minimum experience standards with an approved list of certifications, centrally managed. Questions arise about whether certifications should be valued at the European or national level, with examples like OSCP and CRTE mentioned, or if national TLPT authorities should define them. ENISA or competent authorities should maintain a list of qualified companies and clear certifications for threat intelligence and red team testers at the EU level. Concerns include the potential obsolescence of the TIBER EU Service Procurement Guide without an EU TLPT certification program, and the need for more clarification on valued certifications for threat intelligence teams. A harmonized approach across Europe is recommended, with accreditation processes like CREST's for CBEST suggested, and a validated certification list for selecting independent testers requested.	It is not possible to recommend certificates in the RTS. The TIBER-EU procurement guidelines will be updated to be in accordance with the the requirements of this RTS. Centralised accreditation not in the ESAs' mandate.	No change.

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
Confidentiality of references	The requirement of references may be problematic, as not all tested entities want to be mentioned due to confidentiality issues. There is a legitimate requirement for secrecy and providers may not be able to divulge past exercises. Could TCT provide references in anonymised form?	Confidentiality is mostly a concern for ongoing TLPT and much less so for past TLPT. There is no requirement for TCTs to provide references for past engagements.	No change
Too strict criteria: local providers may be excluded	Very few non-english speaking providers are out there and this proposal would limit that market even further	Some flexibility has been given to allow FEs, on an exceptional basis, to procure testers and TI providers that do not satisfy to all of the requirements subject to adequate risk management measures and agreement of the TLPT authority.	Change in Article 5(3).
The requirements are too vague (4)	- How shall the requirements be validated? - Mechanism to validate references would be needed - It is not clear which red teaming exercises count as "threat intelligence led" except for official TIBER and CBEST tests. - The criteria selection of external testers who are allowed to carry out these tests must be specified (only the number of years of seniority is mentioned in the text).	The requirements are to be validated to the extent possibly by the FE. Years of experience may not be a perfect measure for skill and seniority, but they are a pragmatic compromise which is relatively easy to verify.	In Article 5(2), the requirement for threat intelligence led red teaming has been altered to "red teaming and penetration testing".

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
	Objective criteria should be proposed in the RTS. The scope of recent involvement of individual Red team members in conducting TLPT activities should be checked rather than years of experience.		
The requirements should be stricter	the RTS should include clear minimum requirements related to past projects, team seniority, and certifications. It is emphasized that incident management, including backups, DR plans, and BCM plans, are as crucial as experienced testers. Additionally, external testers and threat intelligence providers should demonstrate experience in TLPT specifically within the financial sector. Each team member should also possess at least one cyber threat intelligence certificate.	The requirements are already considered as too strict by the majority of the respondents.	No change.
Using internal TI analysts should be allowed	It would be relevant to consider that organisations should be able to use their own members of their threat intelligence functions (which is typically present in larger financial entities).	Neither DORA nor the RTS prevent the use of internal TI as long as it is in addition to external TI.	No change
The authority being able to object to the	The potential for objection may constrain the FE's flexibility to utilize external testers and threat intelligence providers. This limitation could result in	The timeline of a TLPT will be reviewed on a case-by-case basis in agreement with the TLPTA.	No change

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
providers is problematic	increased time and testing costs or cause delays in the TLPT process. . If the test is delayed, for example because the authority does not approve the providers, how will be ensured that the test remains on schedule? .		
Involvement of the TPP in selection should be considered	ICT third-party service providers should be sufficiently involved in the selection of any external testers, internal testers or threat intelligence providers assisting with TLPTs over the services of such ICT third-party service providers. The suitability of the testers should also be considered for when an TPP is involved, in this case the suitability might depend on different parameters.	If needed ICT TPP staff can be part of the control team (Article 1(1); in case of pooled test, the ICT TPP will directly contract with the external testers (Article 26(4) of DORA)	No change.
Confidentiality as a requirement for the contractual obligation for the providers	The RTS lacks a clear, comprehensive set of confidentiality obligations for all persons who may receive information concerning a test – threat intelligence providers, testers, national competent authorities, financial entities, service providers.	Article 55 of DORA lays down an obligation of professional secrecy on the staff of authorities covered by this regulation. According to Article 4(2)(d) of the draft RTS, FEs shall "establish organisational and procedural measures ensuring that (…) arrangements relating to the secrecy of the TLPT, applicable to staff of	No change.

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
		the financial entity, to the staff of relevant ICT third party service providers, to testers and to the threat intelligence provider are in place".	
Possibility for FE to delay if cannot procure	FE should be able to delay TLPT to ensure proper procurement	A FE cannot delay a TLPT on its own, as the frequency of the TLPT as their individual starting point is set by its TLPT authority. Any delay would be subject to an agreement from the TLPT authority. In addition, note that some flexibility has been given to allow FEs to procure testers and TI providers that do not csatisfy to all of the requirements subject to adequate risk management measures and agreement of the TLPT authority.	Change in Article 5(3), second paragraph.
Other measures	Suitability can be judged by presentations to TCT and entity to evaluate comprehension. Align further with TIBER-EU SPG / More guidance needed Providers should be treated as ICT TPP CAs to maintain a list of providers and grant accreditation/certification	Suitability must be based on verifiable, objective criteria. Further alignment with the TIBER-EU procurement guidelines will come when these procurement guidelines will be updated. Competent authorities do not have the mandate to act as accreditation bodies.	No change

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
External testers and threat intelligence providers	- RTS should allow for threat intelligence provider and testers to be the same provider. - RTS should include possibility for threat intelligence provider to be internal if FE is mature enough or there is segregation between TIP and internal testers. - Possibility to use intragroup TPP as TIP, under same requirements as external TIP, as they truly understand the FE's business. - Clarify if external threat intelligence provider can be a TPP with whom the FE or its group already has arrangements with. - Proposal to allow the threat intelligence provider to communicate with any internal resources that could allow the formation of a more targeted threat plan. - Clarify definition of external tester: are testers from another legal entity belonging to the same group of entities considered external? - The RTS should specify the independence conditions that the threat intelligence provider	Additional requirements on conflicts of interests have been introduced for both threat intelligence providers and testers.	Changes in Article 5.

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
	and the red team must respect to be considered external to the audited financial entity. - The RTS should specify the exact independence criteria between the threat intelligence provider and the red team if an external service provider provides both Threat Intelligence and Red Teaming services - It could be that a pentester is hired to work internally from a security company. It is not clear through the text whether this person would still be seen as an internal tester.		
Assessment of certification	FEs will not be able to to monitor the effectiveness of the certification or qualification. Clarify what is a reference and how the FE can challenge the testers. FEs are responsible for compliance, not CA.	FEs are responsible for determining what constitutes a reference and for monitoring the effectiveness of the certification and qualification provided.	No change.
Restoration by TIP	In Article 5(2)(g) better clarify the "restorations" threat intelligence providers must do.	Article 5(2)(g) requires testers and threat intelligence providers to carry out certain restoration procedures. This list is left open as ex ante there is no predetermined list of what could all fall under "restorations".	No change.

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
Option to postpone TLPT if no tester procured	Article 5(2)(j):"If the control team is unable to procure external providers that meet the requirements of Article 5, it shall notify the TLPT authority and consider postponing the TLPT until the procurement guidelines can be met."	In agreement with the TLPT authority under exceptional circumstances, a postponement can be a possibility.	No change.
Optionality of risk management measures	Include optionality for financial entities when listing requirements in Article 5(2) paragraphs (a) to (g). The draft text in Article 5 paragraph 2 should hence be amended with "The control team shall consider taking measures to manage risks…", instead of "The control team shall take measures…".	Due to the sensitive nature of TLPT, establishing risk management measures is a key aspect of the preparation of a safe testingprocess. This constitutes the baseline for TLPTs.	No change.
Testers can also act as threat intelligence provider	Clarify whether the threat-intelligence provider can act as the tester, as is common practice across the sector. RTS should ensure this can remain common practice. TIBER does not mandate that the threat intelligence provider and the red team provider should be distinct	Threat intelligence providers and testers may come from the same provider, but the teams must be independent.	Article 5(2), points (e) and (f), now includes the requirement that TI and testers must be independent from each other if they come from the same provider.
Bar the threat intelligence provider from receiving scoping information	It is unclear why provisioning of such confidential information back to the TI providers is necessary. We suggest excluding the TI provider from this requirement.	In accordance with TIBER-EU.	No change.

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
There should be requirements for the providers' organisations themselves	As delivering modern advanced red teaming / TLPT exercises requires more than just 2 testers and a manager; these people need support from a capability development perspective (i.e. creation of novel tooling to bypass constantly changing security protections) and in providing a secure, resilient, test-specific red team infrastructure from which to test from. The current provisions place a requirement on the testers, but not on the firm/ organisation providing the test; it should.	These requirements were selected to be in accordance with TIBER-EU	No change
Include ICT TPP in control team to select providers	A respondent proposes to include the TPP in the control team so that they have a say in the selection of the providers	If deemed necessary, the ICT TPP can also be a part of the control team. In pooled testing, the ICT TPP is in charge of hiring the providers according to L1.	No change
FEs should be encouraged to share experiences with their peers regarding providers	the knowledge and skills of providers by the years of experience is not ideal, but currently within Europe there is no better way to assess this. I would suggest to financial entities undergoing TLPT to not shortlist their provider by the number of years experience alone, but to also check with their peers in order to assess real world experiences they have had with them. This will also vary with time because	It is not up to the ESAs to mandate such an exchange of experiences in an RTS.	No change

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
	experienced red teamers change providers and take their experience with them.		
Indemnity Insurance	Full indemnity insurance may also not be possible for most providers.	Article 27(1)(e) of DORA already requires testers to be "duly and fully covered by relevant professional indemnity insurances, including against risks of misconduct and negligence"	No change
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.			
Years of experience an appropriate measure	Many respondents indicated that they viewed the specified years of experience for external testers and threat intelligence providers as being an appropriate measure to ensure external testers and threat intelligence providers of the highest suitability and reputability and the appropriate knowledge and skills.	No change necessary	No change
Alternative qualitative criteria based on expertise and market conditions	Respondents expressed concerns about imposing strict experience requirements for external testers and threat intelligence providers in TLPT, noting that this could negatively impact highly-skilled individuals with less experience.	It is acknowledged that quantitative criteria will have this shortcoming. However, quantitative criteria have a number of other advantages, such as being objective, measurable, reproducible, simple, consistent and comparable. Overall, the	No change.

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
	Many suggested that years of experience do not necessarily reflect true expertise, qualifications, or aptitude. Instead, they proposed that requirements should correspond to necessary expertise and market conditions, ensuring suitable entry barriers. - qualitative criteria and a right of veto for the TLPT Cyber Team. - principle-based approach, requiring a proven track record rather than a set number of years. combining years of experience with education, expert training, and previous testing experience.	RTS retained these quantitative criteria for testers and TI providers.	
Alternative criteria: number of previous TLPT/TIBER-EU tests	- Suggestion to replace number of years to be replaced by a set number of TLPT/TIBER-EU tests, with many recommending a minimum of three. Respondents emphasized that references from previous threat intelligence-led red team tests are crucial for assessing the suitability, reputation, and expertise of threat intelligence providers and testers.	The requirement for references from previous assignments has been retained, but it had to be broadenend to allow for experience in red teaming and penetration testing. Limiting the experience to only TIBER-EU/TLPT would have been too restrictive at this point in time.	Modification of Article 5

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
	- references should focus on individuals rather than provider firms. - Call for mechanisms to validate confidential references clarity on which types of assignments would meet the requirements for both threat intelligence providers and external testers.		
Requirements should be stricter	Some respondents suggested that: - each threat intelligence team member have at least three years of experience, - red team staff have at least five years in the financial sector. - TLPT team leads complete five TLPT engagements and team members complete two. - references from at least three previous TLPT assignments. Further recommendations included adding certifications, continuous learning, expertise in relevant areas, education, training, previous	As the majority of the respondents indicated the opposite, this was not included in the RTS	No change

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
	testing experience, and financial industry knowledge.		
Too strict requirements will limit the market	Overly strict requirements could shrink the market, leading to higher prices and limited availability of providers and constrain firms' ability to acquire skilled professionals and make it difficult to find qualified external vendors. Some suggested replacing "years of experience" with "sufficient expertise" to allow financial entities to decide on the qualifications of external testers and threat intelligence staff. They emphasized that barriers to entry could prevent new providers, who offer fresh perspectives, from entering the market. Flexibility in experience requirements for threat intelligence teams during the initial years of TLPT enforcement was also recommended to allow providers to gain experience. Additionally, it was suggested that requirements focus on personnel rather than organizations to avoid deterring new providers. Some respondents expressed concern that the requirement for years of experience would be difficult to fulfil by local providers within their	It is acknowledged that this may be a concern. Hence a possibility was introduced to allow FEs to hire providers who do not meet this criteria, provided that they accept and as necessary mitigate the additional risk this introduces. See response to Q 7	Modification of Article 5

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
	Member State(s), in some cases borne by the perspective that local language skills may be relevant for both threat intelligence and external providers.		
Requirements should be calibrated to market availability	Some respondents suggested for the ESAs to initiate a study of the provider market to ensure there are sufficient threat intelligence and red team providers fulfilling any posed requirements available for entities to procure for TLPT. These respondents considered market availability of qualified resources a crucial factor in calibrating and setting the correct thresholds as requirements for threat intelligence providers and external testers.	The timeline did not allow for market studies	No change
Guidelines would be more appropriate than RTS requirements	There are no single metrics which can easily summaries if a tester is suitable. A combination of factors such as, but not limited to, professional certifications, breadth of experience across different sectors, specific skills relevant to emerging cyber threats, and a demonstrated ability to adapt to the evolving cybersecurity landscape. Hence flexibility should be given.	Given the sensitive nature of TLPT it was felt that guidance alone was not sufficiently strong.	No change

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
Q9. Do you consider the proposed process is appropriate? If not, please provide detailed justifications and alternative wording as needed.			
TLPT process / timeframes	the rigid application of timeframes in the process should be changed, especially on red team testing, which go beyond the TIBER expectations and fail to provide discretion for the financial entity to react to unforeseen events or delays.	RTS timeframes are in accordance with TIBER 2.0	No change.
Reduce TI phase scenarios	The TI phase could be lightened to only include one or two scenarios (for instance based on generic threat) while the purple teaming phase could be strengthened to have a collaborative approach on how to increase their detection and response systems and processes.	RTS is in accordance with TIBER 2.0, which will require the execution of three scenarios. The ESAs welcome the positive feedback on purple teaming. The FEs are welcome to extend their purple teaming activities on a voluntary basis beyond the requirements of the RTS.	No change.
Red team phase duration	The duration of the active red team phase should be proportionate to the scope of the exercise and the complexity of the FE, taking info account potentially unplanned events. This could be reflected either by adjusting the relevant timeframe or removing it completely	RTS timeframe for active red teaming is in accordance with TIBER 2.0	No change.
Critical Systems	Paragraph 42 of the public consultation references "critical systems". This is an undefined term and is not used within the DORA Level 1 text.	The ESAs welcome the feedback. Wording has been amended.	Change. "critical or important function" in paragraph 51 of the final report.

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
Timeline Closure Phase: Increase time to prepare blue team test report, test summary report, remediation plan	Increase the relevant timeline foreseen for the preparation of the test summary report, blue team test report and remediation plan. A high number of respondents highlighted that the maximum of 4 weeks to draft the blue team report is too short, given that this activity cannot be planned as the blue team is not aware of the ongoing test. Respondents also comment that this short term planning could monopolize the blue team, leaving the institution less bandwidth to detect and respond to real incidents. Some respondents would like to see this step increased to 8 or even 12 weeks.	The ESAs have reviewed the timeline in particular of the closure phase, to allow for additional time.	Change. Recital 22; Art. 9 (4-7); Art. 10 (1)
Potential duplication of work / Sharing the test summary report along remediation plan	Propose that the test summary report be shared together with the remediation plan, and not in advance as proposed in Article 9(7).	The RTS does not prohibit the FE from submitting both documents at the same time. While Test summary report and remediation plan are two separate deliverables, they can be submitted simultaneously, if desired by the FE.	No change.
Scenario weighting	It seems that the number of scenarios and targets are given independently of the results of the TI phase. We propose that certain scenarios be weighted higher depending on the results of the TI	In accordance with TIBER-EU 2.0, 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 control team shall then select at least three scenarios.	No change.

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
	phase and that other scenarios be made optional as a result.	There is no weighting of scenarios in TIBER-EU or the RTS.	
Responsibilities of Control Team and Testers regarding the testing process	Article 6 paragraph 7: testers should inform control team about testing process to be followed	The control team remains ultimately responsible for the conduct and risk management of the test. It is the control teams responsibility to inform the testers and threat intelligence providers about the process to be followed.	No change.
Escalation chain	Article 4(2) under c of the RTS states that the control team is informed of any detection of the TLPT Besides the TLPT team, nobody within the company (the tested entity) knows about an ongoing TLPT. The control team cannot be informed if staff members have detected a TLPT.	The control team shall be set up in a way that allows involvement in the escalation chain in case of an incident. The TLPT authority validates the control team composition to ensure adequate staffing.	No change.
Use of already contracted TIs	FEs can use already contracted Tis to select relevant scenarios and does not have to be part of the process, if one already has threat intel services running.	In accordance with TIBER-EU, the TI Provider shall be external to the FE. If the FE has already procured an external TI Provider thatis sufficiently qualified to execute a TLPT as laid out in this regulation, this RTS does not prohibit the use of such a TI Provider, as long as it is external.	No change.
Purple team excercises	Purple team tests should be encouraged when possible but not mandatory / flexibility when to be performed. Clarification needed on mandatory	In line with TIBER-EU 2.0, purple teaming is a mandatory element.	Change. Art. 9 (5); Recitals 21 & 22

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
	purple teaming in the closure phase, as it might duplicate the work. Expectations, duration, and deliverables for the purple teaming step are deemed unclear by some respondents. Others feel that the PT would not add learnings compared to the RT and propose to make PT optional. The following passage is found to be unclear and should be reviewed: "may agree on whether to repeat specific parts of the TLPT and/or on carrying out purple teaming exercise".	Purple Teaming in the closure phase has a different focus than purple teaming in the testing phase. Recital has been drafted to elaborate on expectations for purple teaming during the testing phase and the closure phase. The referenced passage that was perceived to be unclear has been deleted.	
Testing of sub-contractors	Testing is only feasible with direct contracting parties. Financial entities should not be required to test further down the subcontracting chain. The RTS should clarify this.	Testing scope will heavily depend on individual analysis of outsourcing arrangements. No general statement can be provided.	No change.
Leg-ups	- The control team shall provide leg-ups based on the red team test plan in a timely manner. - The TLPT authority should be informed of, but not required to approve, any leg-up adaptations or additions. - Leg-ups should be limited to the financial entity's own environment, not third-party	In accordance with TIBER-EU, the test manager is heavily involved throughout the process. Provision of additional leg-ups may fundamentally change the TLPT. Hence, approval is required. Each TLPT is different and leg-up provisioning needs will vary. It is not possible to provide a blanket statement that leg-up provision will be	Change, clarification in Art. 8 (8), recital 20 and final report. Change, wording adjusted "and where no other reasonable alternative exists". Art. 1

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
	environments. Clear definitions and examples of leg-ups should be provided in the RTS. - Leg-ups should evaluate a financial entity's security in the cloud, not the security of the cloud. Granting leg-up access to third-party provider infrastructure poses unacceptable security risks. - Information leg-ups should precede access leg-ups, which should be a last resort if no other reasonable alternatives exist. - Define 'pre-requisite' distinctly from 'leg-up'. Recital 18 Amendment: - Insert 'the financial entity's own' before 'ICT system or internal network'. - Add: A leg-up shall be limited to the financial entity's own ICT systems or internal networks and not include access to third-party ICT provider systems beyond what the financial entity ordinarily accesses. Leg-ups should not enable testers to access third-party systems supporting other customers or increase risks to service quality or security for those customers.	limited to FE in any case. All participants are urged to ensure operational stability throughout. 'pre-requisites' for scenarios are no 'leg-ups', but starting points for a scenario.	
TI and scenario definition	Strict scenario testing might not be optimal. Penetration testing, even when performed under TIBER-EU, is a dynamic activity that continuously	There is no specification of a maximum number of scenarios, only a minimum.	No change.

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
	reconsiders scenarios or even identifies new ones as the work progresses. The number of scenarios and targets should never be specified independently of the results of the TI phase Several respondents voice their concern towards the fixed number of 3 scenarios to be executed. Proposals range from only two scenarios, to at the institutions' discretion, to linking the number of scenarios to the findings during the TI phase. Article 7: It should be stated clearly that the general threat landscape provided by the corresponding TIBER-EU unit is an appropriate basis for the targeted threat intelligence report.	RTS allows for one of the scenarios to address 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. In accordance with TIBER-EU 2.0, a minimum of three scenarios is required. In accordance with TIBER-EU the provisioning of a GTL is not mandatory. If a GTL is available, it may serve as the basis of TI.	
Clarify timeline for threat Intelligence phase	Defining threat intelligence phase duration and resources capability for both threat intelligence and red teaming phase. It does not currently define a time range for the threat intelligence gathering phase.	Recital has been amended to address the approximate duration of threat intelligence gathering, in accordance with TIBER-EU.	Change. Recital 16.
Confidentiality	Disclosing vulnerabilities found during TLPT assessments can have several unintended negative consequences, so findings should be exempt due to their sensitive nature. All reports must be treated as	The ESAs welcome the feedback and concern for confidentiality. The RTS refers to necessary riskRisk management measures. Additionally	No change.

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
	confidential by all parties. Ensure appropriate management members are part of the control team, responsible for approving the scope specification document to maintain confidentiality. Authorities should be required to keep reports confidential and outline security requirements for submitting confidential test reports to supervisors. The RTS should allow information sharing from ESAs to other organizations related to TLPTs only with the firm's consent or on a need-to-know basis due to the sensitive nature of the activity.	Article 55 of DORA clarifies professionalProfessional secrecy for authorities.	
Roles and responsibilities: Control team and test managers	Article 4.2.b. should be amended to reflect that the control team should inform rather than consult test managers. Several respondents emphasise the risk of an intense involvement of the TCT and TLPT atuthority in the TLPT process, especially in the light of approvals of changing plans, introducing leg-ups, or reacting to detection from the blue team. Delays due to an overly consultative model and without deadline for the various approvals from the authority are mentioned as risks to consider.	Involving members of the blue team could result in loss of confidentiality and hence requires diligent care. In line with TIBER-EU, no change has been made.	No change.

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
Test suspension	Article 8(10): ICT third-party service providers should be considered when deciding on a test suspension.	The RTS does not forbid FEs from involving its ICT third-party service provider in this decision. The decision remains with the control team lead, subject to approval by the TLPT authority.	No change.
Length of the active red team testing phase should be more flexible	Many respondents noted that the proposed 12-week minimum in the RTS does not consider factors like institution size, complexity, and scope. They suggest a lower minimum, such as 6 weeks, or aligning with the TIBER-EU framework's 8 to 10 weeks, or leaving the duration to the institution's discretion. More flexibility is desired, with some proposing a maximum of 16 weeks to keep the test manageable. Concerns include the timeline being too long and costly. Respondents also want clarity on the dependency between the red team testing phase and purple teaming elements, especially if detection shortens the 12-week period. In such cases, remaining time spent in purple teaming should count towards both the 12-week minimum and the mandatory purple teaming. Similar proposals apply if objectives are met before 12 weeks.	RTS timeframes are in accordance with TIBER 2.0, hence, no change was made with respect to the length of the active red team testing phase. The dependency between the length of the active red team testing phase and the purple teaming element has been clarified in the RTS.	Change. Clarification of Article 8 (10).

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
Clarify what should be done during red team testing phase	A number of respondents point out that the 12 weeks of active red team testing phase only mentions duration. There is no mention of the effort, the numbers of scenarios in this 12 weeks period, or the level of quality to be expected. Clarification is needed as to how cooling-off phases or interruptions of scenarios are being counted towards the 12 weeks.	The 12 weeks cover all scenarios. The timeframe is not per scenario. The 12 weeks allow to mimic stealthy malicious actors and the effort needed will depend on the chosen scenarios. As for the quality of the TLPT, this is covered by the expectations for testers	Change. Clarification has been done in Art. 8 (5).
Preparation phase	Some clarification is requested around the deadline for procuring the TI supplier and testers. On the same topic, other respondents understand that the procurement should be done within the preparation phase, but that 6 months could be too short in case of scarcity, worsened by the perceived dependency between the initiation documents and the procurement. Three months is considered to be too short to allow for proper preparation and come to an agreed and comprehensive initiation document package, especially as other tests or activities might be already planned in that period. The possibility to defer or discuss the first deadline between the institution and the authorities should be made possible.	Procurement can be prepared, but not finalized, upfront, and thus before finalisation of the initiation documents. The text reads "following the validation" but does not prohibit to already start sooner. The possibility to request extension towards the TLPT authority is always provided. Final Report urges Authorities to contact FEs before the official "notice". Once to inform that an institution is in scope, and a second time ahead of a notification to be able to plan and budget. It is recommended that FEs start preparing for a TLPT as soon as they become identified.	No change, but clarification in the final report.

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
ICT TPP identification – duplication in Annexes I and II?	Some respondents point out that the list of ICT TPP that support critical or important functions is in both scope (Annex II) and project charter (Annex I). The relevance of this duplication is questioned.	Annex I is referring to critical or important functions, while Annex II is referring to ICT systems, which are underpinning the critical or important functions.	No change.
Exceptional circumstances	More guidance is requested towards what "exceptional circumstances" mean, and when and how to react. Taking into account the potential impact on third parties is requested to be specifically mentioned in the decision to suspend/halt a test.	"Exceptional circumstances" may vary from case to case. It is perceived to be dangerous to limit them to specific events. RTS allows for discretion of control team lead but ensures validation by Test manager.	No change.
Restrictions for testing TVs in production	Respondents point out that trading venues are bound by MiFID II to "not test in production", nor during the normal working hours.	DORA = live prod systens Normal working hours issue could be considered in the risk assessmsent and risk management measures for the trading venues in scope of TLPT.	No change.
Other (timelines)	- Shorten BT report to 3 weeks - Shorten replay to 2 weeks - Proposal for all documentation no later than 10 weeks after the end of the active red team test phase - PT needs to be longer - Weekly reporting too frequent	The majority of respondents voiced contrary opinions.	No change.
Follow up	Clarity on follow-up of remediation plan reco's (and impact on next cycle)	Follow up on TLPT is outside of the scope of this RTS, as it is a supervisory task.	No change.

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
Other (general)	- Management body part of control group vs "informed" - Take into account industry best practices, certifications, standards… - Test summary should be shared (portions) where relevant with ICT TPP's - ICT third-party service provider staff should remain part of the control team	The RTS does not prohibit FEs from doing so.	No change.
Definition for Red Team	Red team should also be defined in the RTS	Testers defined in DORA.	No change.
RTS and TIBER to be melted into one / harmoinsation	TLPT and TIBER-EU should be merged into an identical test method with identical terminology, requirements, procedures etc. RTS should harmonise with existing national cybersecurity and audit requirements to avoid duplication of efforts and to streamline the TLPT process.	RTS is binding. TIBER-EU provides additional guidance and best practices. Further harmonisation with national cybersecurity and audit requirements is beyond the scope of this RTS.	No change.
TLPT process	Critical vulnerabilities identified during TLPT should be immediately (or at the very least, without undue delay) shared with the control team and blue team, ensuring timely remediation. Separate versions of	Rules of Engagement between testers, Threat Intelligence Provider and Control Team may be organized at the discretion of the FE. The RTS does not prohibit FEs from enforcing immediate information on vulnerabilities by testers, nor does	

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
	the red team report may be needed when an ICT ICT TPP is involved. Include in the templates a summary assessment of the type of actionable intelligence that threat intelligence providers should look for when preparing the threat intelligence report.	it prohibit multiple versions of the Red Team Test Report, nor does it limit the sources of TI.	
Automated testing	DORA does not provide any automated testing mechanisms that could streamline the testing process, while maintaining the principle of human in the loop.	Red Teaming may contain automised elements, e.g. automated port scans. However, red teaming in general is not associated with automised testing.	No change.
roles and responsibilities	The roles and responsibilities of all parties should be clearly defined in the preparation phase.	The RTS does not prohibit FEs from clarifying roles and responsibilities beyond the definition of roles and responsibilities, provided in the RTS.	No change.
Content of summary test report	The test summary report should include: further details on whether common ICT systems have been tested that are equally used by the FE in other Member States and information on common defensive capabilities	The RTS does not prohibit FEs from including these details in their test summary reports.	No change.
Control team	Article 1 Definition: Control Team: The team composed of staff from the tested financial entity, including a C-level member, and staff from its third-party service providers, also including a C-level	Composition of Control Team is subject to the decision of the FE and needs to obtain approval from the test manager.	Change. Test manager now validates the composition of the control team. Art. 6 (4)

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
	member if needed, who know about and manage the test. Proposed Edits to Article 4(1): When ICT third-party service provider staff are included in the control team, the financial entity must allow the provider to appoint its own control team lead responsible for its staff's actions within the control team. Additional Considerations: The control team may not have access to every ICT system. The control team should include both Red and Blue team leads to enforce test parameters. Individual exceptions on TLPT information should be granted for procurement experts under TLPT authority supervision.		
Denial of service (DoS) attacks	Recommend keeping denial of service activities out of scope. Propose adding two sub-paragraphs prohibiting: (vi) Acts adversely impacting the quality or security of services by an ICT third-party provider to	The RTS indicates that "unauthorised destruction of equipment of the financial entity and of its ICT third-party servive providers" is prohibited. In addition the RTS does not prohibit the CT from clearly defining DoS attacks to be out of scope for the TLPT.	No change.

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
	customers outside the regulation's scope, or compromising the confidentiality of related data. (vii) Denial of service attacks on the live production systems of a financial entity.		
Q10. Do you consider the proposed requirements for pooled testing are appropriate? If not, please provide detailed justifications and alternative wording as needed.			
Support for pooled testing requirements	Many respondents consider that the requirements for pooled testing are suitable.		Clarifications have been brought across the RTS.
Clarify definition of pooled testing	The RTS is not clear on what pooled testing is, what the rationale behind it is, when and why it should be used, how it should be initiated and what the scoping and process should look like	Pooled testing is defined in Article 26(4) of DORA. The RTS specifies certain aspects of the process (risk management process, testing process with the coordination of several FEs) as well as supervisory cooperation measures necessary in respect of such test when several TLPT authorities are involved (cross-border cases).	Changes in particular to Articles 6, 7, 9 and 14.
Pooled testing should not be further specified in the RTS	- There remain significant practical, contractual and operational difficulties that have resulted in the industry viewing	The RTS specifies aspects of the methodologuy and process which should be followed in case of pooled tests.	New articles 6 and 7, as well as clarifications in Article 14

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
	pooled testing as a theoretical prospect but not, currently, practically achievable. - It is appropriate that the RTS does not prescribe the pooled testing process in detail as this will vary for each test. - given that there is no existing (TIBER) guidance on pooled testing, the RTS should not explicitly regulate pooled testing but guidance should be developed within the TIBER community first.		
Suitability of ICT TPP in pooled testing	- pooled testing is only suitable for generic software solutions that are not customised or hosted in a client environment. - the type of service affects the suitability of the ICT TPP for pooled testing. For example: an IaaS ICT TPP can include the IaaS layer in a pooled test, but a SaaS that services multiple costumers from the same infrastructure cannot. - one pool is not likely to cover all the services bigger ICT TPPs offer to all their client FEs, the RTS should be clear how these ICT TPPs	The ESAs would first like to recall that DORA is meant to be technology neutral. According to Article 26(2) of DORA, the scope should include "all relevant underlying ICT systems, processes and technologies supporting critical or important functions and ICT services, including those supporting the critical or important functions that have been outsourced or contacted to ICT third-party services providers".	No change.

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
	should be treated (how often they should be tested/ what should be tested etc.). - certain (smaller) ICT TPPs might not be able to conduct a pooled test, or at least not with all their FE clients. - the RTS should provide wider requirements for pooled testing. For instance, an industry-wide infra testing of critical service providers would avoid the exercise being done individually for all undertakings, overburdening the providers and generating additional costs to undertakings without any benefit.		
Contractual challenges regarding pooled testing	- most contracts between FEs and ICT TPPs do not foresee TLPT, thus pooled tests would require additional negotiations. This could severely slow down the process of the TLPT as these negations would be likely to happen during the preparation phase of the test and other stakeholders like the TI provider and the external testers could also get involved.	Indeed, the ESAs note that Article 30(2)(d) of DORA requires that the contractual arrangements on the use of ICT services supporting critical or important functions to include the obligation for the ICT TPP to participate and fully cooperate in the FE's TLPT as referred to in Articles 26 and 27.	No change.

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
	- that securing these contractual rights will be difficult to achieve as it amounts to a carte blanche right that could later violate the security policies of the third-party provider. It is worth noting that the scenario and specifics of the TLPT will not have been determined in prior negotiations nor specified within a contract.		
Decision to launch a pooled TLPT	- it is not clear how a pooled test is triggered/ initiated - Pooled testing should be encouraged - proposal: Article 6(4a): "To the extent the scope specification document envisages the testing of the services of an ICT third-party service provider, the financial entity and TLPT authority shall consider whether that testing should be conducted through a pooled test in accordance with Article 26(4) of Regulation (EU) 2022/2554". - the TLPT authority should decide when a pooled test should take place. - the TLPT authority must coordinate with each other and the FEs and ICT TPPs to decide when a pooled test is conducted and with whom.	It has been clarified that where FE intends to conduct a pooled test, its TLPT authority shall assess its relevance, if necessary with other TLPT authorities involved (if financial entities are established in different Member States).	Clarifications in Article 14(4).

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
The FEs in the pool	- there should be more guidance on who should be the designated FE - for cloud services: the ICT TPP should identify every 3 years which services are used by financial entities so that those can be included in a pooled test. - FEs should not be forced to participate in a a pooled test.		
Pooled testing for groups	- for FEs that are within the same group and share ICT services, they should be allowed to do a a pooled test as a group (either on an internal or external TPSP). - clarify if pooled testing if suitable/ allowed for intragroup tests - pooled testing is only suitable if all financial entities are part of the same financial group. - financial entities not belonging to the same group shall be able and allowed to conduct pooled testing jointly, as long as these entities are using common ICT systems or the same ICT service providers. To enhance	Article 26(4) of DORA limits pooled tests to cases where the test could have an adverse impact on services provided by an ICT TPP to its clients that are not financial entities, which might limit the use of pooled test for groups Additionally, the RTS defines and addresses the case of joint tests, for TLPTs other than pooled tests, involving several financial entities using the same ICT intra-group service provider, or belonging to the same group and using common ICT systems.	Definition of 'joint TLPT' (Article 1) and related requirements in terms of process (Articles 6 and 7) and supervisory cooperation (Article 14).

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
	clarity, we suggest explicitly including such a provision in Article 12 of the draft RTS.		
Scope of pooled test	- clarify what the scope of the pooled test should be. - it is not possible in one test to test both the infrastructure of the ICT TPP and the FEs in one big pooled test. The test at the ICT TPP should only be either one scenario used for the TLPT at each individual FE, or it should be the in-phase of one or multiple scenarios for the TLPT of the FE. The test at the ICT TPP should not be the full TLPT for all the entities in the pool. - the scope at the ICT TPP should only include infrastructure that is used by FEs subject to DORA, or other if they explicitly agree. - the RTS uses the concept of third-party providers who "support" CIFs, without any materiality threshold. Financial entities use a significant array of third-party providers to support CIFs. This could result in an impractically larger number of TPPs being included in the scope of the TLPT.	The ESAs consider that in case of pooled (or joint) TLPT it is important that not only the ICT service provider's but also the FE's systems are tested, so that no FE remains untested for up too many years. It has therefore been clarified that for a pooled (or joint) TLPT, at least one attack scenario should focus on the ICT service provider's system while the other scenarios should focus on the FE's system. The scope will be validated by the (lead) TLPT authority.	Clarification on scenarios in Article 9(4).

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
TLPT process for pooled testing	- the TLPT process as described in the RTS is very complicated to follow in a pooled test (which is more complex, with a larger number of stakeholders). The RTS is not clear how this should be managed or what timelines are to be maintained. - the RTS is not clear if the normal testing process should be followed for a pooled test, or to what extent. - principles (guidance) on the interaction between the FEs and the ICT TPP would give clarity, legal certainty and create efficiency. This should also address who is in charge of the test, and how decisionmaking works. - recommend a new Article 8(10a): "Under circumstances triggering risks of impact on quality or security of services delivered by an ICT third-party service provider, the control team lead must suspend the TLPT insofar as it triggers those risks and consider continuing the TLPT using a pooled testing exercise as described in	Clarifications have been brought in respect of the specificities of applying a TLPT process to pooled test, which should follow similar steps as an individual test.	New Articles 6 and 7, changes to Article 9.

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
	Article 26(4) of Regulation (EU) 2022/2554". - it should be clear how flags are defined for pooled tests. - the RTS should make clear if the TI phase at the FE should be the trigger for the pooled test (or participation therein). - purple teaming that includes multiple FEs and TPPs does not make practical sense.		
Risk assessment in pooled testing	- The inclusion of TPPs in a TLPT, or a pooled test scenario, create significant uncertainties about how liability and risk management should operate in practice. For example, the FE's control team will not be able to conduct the risk assessment required in RTS Art. 5 or to manage the risks. If a control team is formed between all participants, it becomes unclear where responsibility ultimately lies for any impacts resulting from the test. This uncertainty is likely to serve as a significant barrier to contractual agreements between the FE	It has been clarified that each FE participating in a pooled test shall conduct its own risk assessment and shall establish risk management measures at its level. In addition, the control team of the designated FE shall conduct the risk assessment and coordinate risk management measures for the "common" aspects of the pooled TLPT.	New Article 6

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
	and various other parties, whether TPPs or other FEs. - The RTS places all accountability of any form of test on the individual FE and therefore pooled tests cannot achieve the risk management requirements nor the practical ability to adhere to the RTS. - Clarify who should determine that ICT TPP impacts several FE to participate in a pooled testing. FE may not know. - Special care to be taken in the risk management of the test as services of ICT TPP may affect multiple entities. E.g. a tester compromise a user account that is known to have administrative rights to disrupt the service, then as a safety control, the pathway is stopped at this point rather than a tester making an actual connection to the service. The risk can still be quantified either during or as a post exercise activity whereby it can be measured to determine if an attacker		

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
	activity or normal user account activity would be logged potentially alerting the ICT provider to the issue. This approach to guardrails should be used on a case-by-case basis, otherwise it could impact overall response measurement.		
Reporting for pooled testing	- It is unclear who should deliver a remediation plan. the findings will not be the same for each entity, thus each entity in the pool should deliver their own remediation plan Follow-up of the remediation will also pose challenges when a ICT TPP is involved. - all forms of report that the FE and any external provider within the RTS are predicated on the individual FE, as per TIBER. It is unclear, however, how all reports will reflect the ICT TPP in a pooled test scenario. - annex III does not make clear whether the TI provider would be expected to apply paragraph 2 to any in-scope ICT TPPs as well as the FE. Doing so would represent a	It has been clarified that unless otherwise decided by the lead TLPT authority, each financial entity participating in a pooled test shall follow each of the steps of the TLPT process: this means that each of them will have to deliver the required reports and remediation plan, unless the lead TLPT authority decides some or all reports can be prepared jointly. The same has been clarified for joint TLPTs.	New Article 7.

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
	material extension of the TIP work and would likely require renegotiation of the TIP contract. - in cases where a group and their internal/ external ICT TPPs have conducted a pooled test, the remediation plan and follow-up should be done for the whole group at once.		
The role of the TLPT authority	- the TLPT authorities should be coordinators of the pooled test - the TLPT authorities should give a speedy approval, coordination between the different authorities should not slow down the pooled testing process. - A pooled testing can potentially cause extended delays as multiple TLPT authorities from the participating FEs consider different requests or information submissions from the control teams. As these approvals are required during the testing phase and involve fundamental elements of the test such as leg ups or actions to maintain confidentiality, delays	Article 26(4) of DORA mentiones to a designated financial entity directing the pooled test, so TLPT here have the same role as in other types of TLPT. Clarifications have been brought as to the designation of the lead TLPT authority in such case. The lead TLPT authority shall consult other participating TLPT authorities which have designated a test manager but will ultimately make the decisions. This should allow for reasonable delays for validations needed.	Changes in Article 14.

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
	could result in breaches to the terms of the test or considerably delay progression of the TLPT.		
The control team	the role, composition and size of the control team for pooled tests is unclear. It should be prevented that the control team gets to an unworkable size.	It has been clarified that the process for TLPT should follow similar steps as an individual TLPT, so each FE shall have a control team in place. The definition of 'control team' has been modified to be able to include "where relevant in consideration of the scope of the TLPT" "any other party" – this allows the designated FE to include staff of the ICT TPP and of other FEs involved in the pooled test, to allow coordination.	Changes in Article 1.
The numbers of requests for pooled testing a ICT TPP can receive	- ICT TPPs are likely to get multiple requests to join a pooled test per year regarding a scope/ scenario that will be similar. - Testing at this frequency is not feasible for the ICT TPPs and will burden the test provider market. It will also make remediation of the findings harder. - It is not clear how finding at a ICT TPP should be treated, and if they could be translated to other FEs if the service they use are the	Supervisory cooperation and the information shared in the attestation delivered to tested financial entities, which includes "where relevant, the ICT third-party services providers that participated in the TLPT", should allow TLPT authorities to coordinate such tests.	Change in the content of the attestation (Annex VIII).

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
	same as the ones that were recently tested in a pooled test. - It does not make sense from a resilience perspective to test the same functions at the ICT TPP multiple times. - The ICT TPP should only have to test their services every three years. Those results should also be used by other financial entities that use the same services. - given the scale of resourcing at stake in such collective exercises, and the level of coordination required, such testing should be valid for a longer period than is the case with regards to non-pooled testing and recommend that testing results from pooled testing be valid for at least a 5-year period, and sit alongside other measures where possible, for example due diligence questionnaires and tabletop exercises. - The ICT TPP should receive something like an independent report that they can use to show other FE clients that they have already		

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
	undergone a pooled test for the same services.		
Cross-border pooled tests	detailed guidance should be given on dealing with TLPT ICT TPPs that operate in multiple Member States and therefore (may) involve multiple TLPT authorities.	Clarifications have been brought as to how TLPT authoriites should coordinate to agree on the limits of the pool, the FE that should be the designated FE and TLPT authority that should be the lead TLPT authority for a pooled test.	Changes in Article 14.
What the pooled test means for the TLPT obligation for FEs	- the pooled test should not be the full TLPT for the FE, thus should not dissolve the FE from their TLPT obligation for that cycle. - detailed guidance should be given regarding determining whether, and if so in which cases, the pooled test releases the financial entity from (part of) its obligation to perform a TLPT. - it should be clear if the FE should also do an additional TLPT for any critical functions that were not covered by the pooled test.	It has been included that even in case of pooled tests, in addition to at least a scenario covering the ICT TPP's, scenarios should also cover the systems of each FE involved in the pool.	Changes in Article 9(4).
Use of testers in pooled test	- the ICT TPP should also be allowed to use internal testers for pooled testing as they have the expertise required to understand	Article 26(4) of DORA provides that the ICT TPP may "directly enter into contractual arrangements with an external tester" so in the ESAs' view this prevents from using testers that	No change.

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
	the ICT TPP systems, services and security posture. - the ICT TPPs internal testers should be considered external testers in pooled testing, as they are external to the FEs.	would be internal to the ICT TPP (as they would not need to contract with such testers).	
Guidelines first	Given that there is no existing practice of pooled testing under the TIBER-EU framework, the ESA's should first draft guidelines, covering: which part (FE or ICT TPP) is in charge of the test, who decides if an FE has to participate in a pooled test, how many remedation plans should be made, how sensitive data and access to systems can be shared within the pool, how indemnity insurances would work.	As for the direction of the test, it is clear from Article 26(4) of DORA that the designated FE shall direct the test, not the ICT TPP. The ESAs have decided to address these points in a high-level manner in the RTS, under the mandate to specify the requirements in relation to scope, testing methodology and approach. It will be assessed at a later stage if guidelines are needed in this respect to ensure better supervisory convergence across the Union.	Changes in particular to Articles 1, 5, 6 and 14.
Concerns with RTS limitation	Wording in RTS goes beyond DORA Art 26. This excludes indirect participation in TLPT by FEs that do not fall under Article 26. current wording in the RTS prevents pooled tests of group-internal ICT third-party providers that work for both Article 26-relevant and non-relevant FEs, as the entire scope of DORA is mentioned as a criterion in the RTS. The scope of DORA Art. 26 would be correct, so that	Pooled testing is defined in DORA. This definition and requirements of Article 26(4) DORA cannot be changed by this RTS. To test jointly financial entities belonging to the same group and using the same intragroup ICT provider or common ICT systems the concept of	No change to the definition of pooled test, clarification of 'joint test' concept (in particular Articles 1, 5, 6, 14).

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
	pooled tests are also possible for ICT third-party providers working exclusively for FEs. The current restriction puts such group-internal ICT third-party providers at a disadvantage and does not apply to less specialized providers. Also in case of outsourcing remediation plans should be under the purview of the ICT TPPs and the relevant competent authority should be involved. it should be allowed to have one pooled testing performed and shared among FE of the same group using the same intra-group provider.	'joint test' has been clarified and related process specified across the RTS.	
Standards and requirements for the use of internal testers 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.			
Not supportive of use of internal testers	- Point of red teaming test is that only publicly available sources are available and used for the simulated attack. Internal testers have inside information and could therefore distort the results and effectiveness of the test. "Social engineering" instrument difficult to use for internal testers in case of red-teaming attack.	The use of internal testers is expressly allowed under Articles 26(8) and 27 of DORA, as well as maximum frequency of use. This cannot be changed in the RTS.	No change.

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
	- Multiple internal testing services may negatively affect security with potential for creating security gaps or breaches. - Recommends using an external tester every other time, every four/five years at the rarest, with internal testing to be conducted on a more regular basis. - question of competence, the effect of routine, conflict of interest, and possible bias.		
Mandate issues	DORA does not authorize ESAs to specify the criteria for external testers	Although this part of the mandate is not explicitly mentioned under Article 26(11) of DORA, the ESAs believe that the criteria applicable to internal testers, as key aspect of the risk management of a TLPT, can be further specified in the RTS as part of the approach to be followed for each TLPT.	No change.
Clarification on mixed teams	Regarding recital 22, a clarification should be added stating that for every third test, "only" external testers shall be contracted, as it is understood that a team of internal and external testers would be considered as a test performed solely by internal testers.	The recital has been clarified in that respect.	Clarification of recital 28.

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
Possibility to use only internal testers	- Use of internal testers should be allowed for every test - for groups: RTS should clarify that one out of 3 tests be conducted by external testers, or if a proportionate approach is required throughout the testing cycle inside the group - [Nside Attack Logic] External test should be mandated on a regular basis	Article 26(8) of DORA expressly requires one out of 3 tests to be conducted by external testers and the use of internal testers is prohibited for credit institutions classified as significant.	No change.
Significant institutions should be allowed to use internal testers	Prohibiting use of internal testers by globally significant credit institutions would fail to leverage the level of expertise which has been carefully developed in recent years within these firms. In the field of cyber risk such expertise is limited and hard-sought.	Such prohibition is made in Article 26(8) 2nd paragraph of DORA and cannot be changed.	No change
Frequency of use of internal/external testers	- Clarify in the RTS if in Article 26(8) of DORA "every three tests" refers to one system or to the FE in general. - Does it mean that a FE would not be externally checked for up to 9 years?	TLPTs are carried out by financial entities so every three tests refers to each TLPT carried out for which a financial entity has obtained an attestation. This frequency results from the combination of comes from Article 26(8) of DORA which requires TLPT to be undertaken by external testers at least every three tests and Article 26(1) of DORA which allows the frequency of tests to be determined by	No change

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
		authority "*based on the risk profile of the financial entity and taking into account operational circumstances*".	
Use of ICT third-part service provider's internal testers	- During TLPT involving ICT TPP: TPP's internal testers have expertise in particular in cloud context, functional operation of their own services and can thus add significant value to an FE's TLPT - Similar to the provisions that apply to financial entities when conducting their own TLPT, ICT third-party service providers should be able to leverage internal testers when conducting pooled testing, where necessary to balance resources appropriately or to ensure the appropriate level of testing rigour (noting that safeguards for internal testers remain, such as prior supervisory approval, the absence of conflicts of interests within the ICT third-party service provider and mandatory use of threat intelligence providers).	Under DORA the concept of "internal tester" is only used in reference to a financial entity, not to an ICT third-party service provider. There does not appear to be a mandate for the ESAs to define requirements in this respect.	No change
Alignment with external testers' requirements	- Clarify criteria on level of experience, and if requirements on certification, experience and previously conducted TLPTs apply to both internal and external testers.	Article 11(1)(d) of the draft RTS cross-refers to criteria for external testers laid down in Article 5(2) of the same draft, so indeed, the same	No change in the RTS but this aspect has been highlighted in the corresponding recital.

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
	- Different treatment of internal and external testers is incomprehensible. Years of employment are not years of experience. - Internal testers should have experience of at least 5 successfully completed TLPTs - Internal and external testers should be subject to largely the same requirements to ensure similar outcomes, especially on experience and certification.	requirements apply to both internal and external testers.	
Too restrictive requirements	Clarify what happens if FE does not find any internal tester respecting all the requirements.	The ESAs believe two requirements can mitigate such risk: - DORA always allows the use of external testers. - Flexibility has been introduced for documented exceptional cases to allow financial entities to use testers not satifying all conditions, subject to establishing appropriate risk management measures (Article 5(3) second subparagraph)	More flexibility has been introduced to contract testers, subject to appropriate risk management measures in Article 5(3) of the draft RTS.
Requirement on past employment period	Remove the requirement. 2-year past employment is unrealistic, other criteria should be considered:	The ESAs acknowledge the challenge but believe a requirement for past employment by the FE should be key to characterise "internal" testers by opposition to external testers, also noting that the	The requirement on past employment period has been lowered to one year instead of two.

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
	- focus on team leader/senior team members to allow more junior members to gain experience - skills, knowledge, experience, relying on the financial's entities' assessment - 2y requirement should be limited to only one member of the testing team - Appropriate red team testing experience should be the main requirement. The RTS should be more stringent on internal testers' knowledge and experience. Clarify that FEs are not required to recruit as a result of this regulation.	use of internal testers is optional and if no internal tester can be found by the financial entity, external testers can be hired. Therefore the possibility offered in DORA to use internal testers is no way a requirement for FEs to recruit such staff.	
Internal testers' policy	- Article 11(1)(a) of draft RTS: Clarify that "*policy for the management of internal testers in a TLPT*" only refers to DORA TLPTs not all other red team tests conducted by a FE. Other testing activities outside of the remit of DORA should not be included within a defined policy. - Clarify training requirements for internal testers: With a centralised accreditation program, FEs would know exactly where to qualify their internal testers	Since this draft RTS is meant to further specify TLPTs conducted in accordance with Article 26 and 27 of DORA, it is already clear this policy only applies in respect of internal testers to be used under Article 27 of DORA only, the ESAs do not see a need to further clarify this here. The ESAs have no mandate to develop a central accreditation program. The ESAs believe requiring that internal testers have "sufficient resources and capabilities" is	No change.

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal

	- Amend Article 11(1)(c) of the draft RTS:
	  ○ include "sufficient time" to ensure internal testers are not occupied with too many other tasks in parallel
	  ○ add obligation for testers to register and document the number of working hours spent on TLPT to ensure proper proportionality and quality is achieved
	- Internal testers' ability to commit to their TLPT tasks should be emphasised in the final RTS: would be unrealistic for internal tester to have to deliver an attack whilst carrying out or being responsible for normal day-to-day business
	- No need for a separate policy for internal testers, should be part of the general policy for TLPT
	- Internal testers may have an advantage over external testers, so scope of work needs to be clearly specified.
		broad enough to cover the need to have sufficient time and can commit to their TLPT tasks.
		
		There is no requirement to have a separate policy for internal testers, nothing in the RTS prevents to have it as a part of the FE's policy on TLPT, if any.
		
		The ESAs want to highlight that in additional to specific requirement, internal testers are also subject to the requirements applying to external testers (cf. Article 13(1)(d) of the draft RTS)	

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
	- Suitability and training criteria should be removed from the policy as they are covered by the hiring process and the job descriptions. - requirements should be more stringent on internal staff by applying a policy for internal staff on top of the DORA requirements, including technological experience etc.		
Addressing conflicts of interests	- Need for additional details on the criteria for using internal testers, especially in terms of conflict of interests (eg. same person cannot provide operational or assessment activity with respect ot TLPT applications/IT systems) - The RTS should specify the set of conditions that the internal RT must verify regarding independence and conflicts of interest. - Strong mechanisms should be set in place to ensure the independence of red-team testers and IT/cyber accountable managers. External control might be put in place to ensure the objectivity of the results. - The draft RTS should include a provision to protect internal testers as they can identify	There is a requirement for the policy on internal tester to address potential conflicts of interest: the ESAs believe this should be defined by each FE and cannot be imposed as a one-size-fits-all requirement.	No change.

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
	vulnerabilities that the company has no interest in disclosing.		
Proportionality in the requirements for internal testers	Proportionality needs to be applied when it comes to internal testing for small and medium entities due to the cost involved or the availably of internal testers. The limitations regarding the minimum size of the internal team could be lowered to a test lead and at least one additional member i.e. a total team size of two.	The ESAs want to recall that the use of internal testers is only an option for FEs, and that external testers can always be used.	No change.
Supervisory cooperation Q12. Do you consider the proposed requirements on supervisory cooperation are appropriate? If not, please provide detailed comments and alternative wording as needed.			
Clarify that TLPT is not a supervisory activity	The RTS should be amended to clarify that TLPTs are not a supervisory activity. In accordance with article 26 and Article 27 in the Level 1 text, it is considered inappropriate that the TLPT Authorities are "to organise" and "to lead" the tests as a TLPT test is an oversight activity. The authorities should review the results of the tests, but	Performing TLPTs now being a legal requirement for FEs, it is effectively a supervisory tool for authorities. However, as highlighted in the recital it should also be seen as a learning tool for the FEs. TLPT authorities do not lead the test itself, which is directed by the tested FE. The TLPT authority involved in a test however validates various decisions and documents produced during the	No change

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
	they cannot both lead a test and evaluate the results of the test in an impartial manner.	TLPT, in accordance with the TIBER-EU framework. The concept of "lead TLPT authority" is meant to designate, in case a TLPT involves several TLPT authorities, the TLPT authority that will coordinate the other TLPT authorities involved and make decisions for all of them during the test.	
Not supportive of cooperation	TLPT authorities cooperation may prove problematic with different levels of engagement, different methodologies, etc.	Article 26(11)(d) of DORA requires the ESAs to specify further "the type of supervisory cooperation, which are needed for the implementation of TLPT…"	Clarifications have been brought as to the cooperation of TLPT authorities in case of pooled and joint TLPTs. The TLPT authorities will assess what is the most appropriate size for a TLPT involving several FEs.
Scope for cooperation and coordination	The RTS should detail the scope, procedures and mechanism (clear and flexible) to ensure a smooth implementation of TLPT test, especially where financial entities operate in more than one Member State or belong to a group (branches and subsidiaries) to avoid duplication.	When a FE operated in several Member States through the freedom to provide services including through branches (ie there is only one legel entity involved) – this is addressed in Article 12(1) of the draft RTS. As only one FE is concerned, the TLPT shall follow exactly the same process as the one described for a FE having no cross-border activity. When a FE belongs to a group (ie several FEs) using the same intragroup provider or common ICT systems, their TLPT authorities can assess whether a joint TLPT can be organised – this is	Clarifications have been brought in respect of TLPTs organised in respect of groups (joint TLPTs) in Articles 6, 7,9 and 14

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
		addressed in Article 12(2) of the draft RTS. the specificties in terms of risk management and process to be followed in such case have been further specified.	
Single leading TLPT authority	The RTS should clarify that there is a single leading TLPT authority as ultimate responsible to coordinate the TLPT process.	In the cases where several TLPT authorities are involved in a TLPT (FE having branches or operating in other Member States, polled TLPT, joint TLPT) one TLPT authority is designated as the 'lead TLPT authority', to coordinate the other TLPT authorities involved and make decisions for all of them during the test.	No change.
Single European TLPT authority	Ultimately, there should be one European entity supervising TLPT testing	This is out of scope of the ESAs' mandate	No change.
Consultation of FEs on involvement of TLPT authorities	The financial entity should: - be consulted about the authorities participating in the TLPT; - select which authority will be appointed as TLPT lead authority; - make initial recommendation to home TLPT authority of which other TLPT authorities should be invited to be involved in the TLPT, home TLPT authority should validate and reach out to host authorities	Although ultimately it will be for the TLPT authorities to decide which FE(s) and which TLPT authorities (and in which capacity) will be part of a TLPT, this assessment will be based on information provided by the FEs envisaged to be part of that TLPT.	The ESAs have clarified the cooperation process for TLPT authorities to follow to participate in a pooled or group TLPTs. Articles 14

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
	and also allow ICT third-party service providers to appoint their own control team lead or have a role in the appointment of the singular control team lead. To the contrary, other respondents supported that members states should determine which other states to involve.		
Number of TLPT authorities participating in a test	The RTS should set a maximum of TLPT authorities participating in a test contrary to what currently indicates "other authorities may only participate as observer". TIBER testing does not scale well beyond 3 authorities. Key factor to multi-jurisdictional test is the extent of centralisation of ICT infrastructure by FE or if there are specific ICT infrastructures for operation in individual MS. Alternative: require FE to conduct separate smaller tests by different TLPT authorities but sufficiently covering critical or important functions across all relevant MS.	The size of a TLPT and number of TLPT authorities involved and in which capacity (test manager or observer) will be up for the TLPT authorities to decide. The ESAs believe this cannot be limited upfront and needs to be assessed on a case by case basis, in order to carry out the most efficient, comprehensive and safe TLPT.	Clarifications on cooperation between TLPT authorities have been brought in respect of pooled and joint TLPTs (Art 14).
Role and responsibilities of participating authorities	- The RTS should clarify whether there will be one lead authority and all other authorities/ host authorities may only participate as observer and define precisely the roles/responsibilities assigned to the supervisory authorities during	TLPT authorities involved in a TLPT to decide among them in which capacity they will take part in the test, either by assigning a test manager or by observing.	Clarifications on cooperation between TLPT authorities have been brought in respect of pooled and joint TLPTs (Art 14).

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
	the execution of joint tests, when TLPTs are performed among several Member States - Clarify that TLPT authorities participating as observers not expected to input on scope of the TLPT	If involved as observer they are not expected to input on the scope of the TLPT. All decisions to be made by the lead TLPT authority.	
Groups: cases to conduct joint TLPTs	- The RTS should clarify in which cases a financial group can perform a joint TLPT. - Joint TLPTs should be performed wherever possible: the RTS should more firmly encourage ESAs cooperation, requiring that a TLPT which can be conducted on a group-wide basis, covering all subsidiaries, under a single lead TLPT authority, should be done wherever possible.	The concept of 'joint TLPT' has been defined to clarify in which cases this possibility can be considered by TLPT authorities. The ESAs believe the launch of TLPT at group level should not be mandated in the RTS as this should always be a case-by-case assessment, involving discussions with the FEs and potentially other TLPT authorities in case of a cross-border group.	Clarifications have been brought in the RTS cf. definition of joint TLPT in Article 1.
Groups: FEs in scope of joint TLPT	The RTS should clarify: - if the TLPT authority of the Member State in which the financial entity group holding is located can autonomously define if and which group legal entities, located in other Member States, shall be involved in the perimeter of the TLPT activities - Collaboration requested to ensure critical functions can be attributed to relevant MS	The TLPT authorities of FEs using the same intragroup ICT service provider will decide among them which FEs shall be included in the scope of the TLPT and in which capacity (lead, test manager, or observer) their TLPT authorities will be involved as well (not all FEs will automatically be included in the scope of the same joint TLPT) . Only the FEs included in the scope of such joint TLPT would benefit from an attestation if the TLPT is deemed copliant with DORA requirements – not	Clarifications on cooperation between TLPT authorities have been brought in respect of pooled and joint TLPTs (Art 12).

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
	- if participation of group legal entities in joint TLPT can be proposed by FE or is it decided by TLPT authority? - how the scope of a joint TLPT will be defined? - in case a FE has an internal ICT provider providing services for all the group's entities across multiple member states, would a joint TLPT validate the TLPT requirement for all the group's entity? Would all the group's entities be involved in the joint TLPT or only a subset?	all FEs using the same intragroup ICT service provider.	
Secure information exchange system	The RTS should further clarify the mechanisms that will be used to ensure effective coordination across TLPT authorities and establish a secure information exchange system for sharing and storing TLPT related information.	Article 55 of DORA (Professional secrecy) applies to "any confidential information received, exchanged or transmitted pursuant to [DORA] shall be subject to the conditions of professional secrecy laid down in paragraph 2" i.e. to "all persons who work, have worked, for the competent authorities pursuant to [DORA], or for any authority or maket undertaking or natural or legal person to whom those competent authorities have delegated their powers, including auditors and experts contracted by them".	No change
Significant credit institutions: TLPTs and TIBER EU	- clarify in which case of significant credit institutions, authorities at the member state level will be engaged as observers, to avoid the	The ECB is the TLPT authority for these FEs (see Recital 2 of the draft RTS). Cooperation between the ECB and national central banks is out of	No change

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
	situation of duplicative TLPT exercises (namely an ECB-led vs existing TIBER framework) - Clarify how cooperation will work for significant credit institutions operating in various MS reporting to ECB but belonging to groups	mandate of this RTS, to be agreed between the ECB and the national authorities.	
Possibility for not involved TLPT authority to recognise a TLPT	The possibility to issue a mutual recognition should not be limited to those TLPT authorities that participate or observe the test: may not have been able to participate or observe (eg. lack of resources) but to avoid having to conduct duplicative TLPT.	For each TLPT, an attestation is delivered only by one authority: the lead TLPT authority. However mutual recognition ensures that all other TLPT authorities will recognise it. Given mutual recognition, no need for attestations to be delivered by other authorities.	Clarifications have been brought as to TLPT authorities' roles in case of pooled and joint TLPTs.
Content of the attestation	Attestation should indicate: - Information on the underlying systems, technologies and infrastructures which were tested in the TLPT - the common ICT systems and relevant defensive capabilities that were part of the TLPT	The attestation shall include information on the critical or important functions that were in scope of the test and among those, those in respect of which the TLPT was not performed. It shall also indicate whether other FEs or ICT third-party service providers were included. The ESAs consider that information ont he systems would go to an unnecessary level of detail for an attestation, also considering that this is very sensitive information.	The minimum content of the attestation has been further detailed in Annex VIII to the draft RTS.

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
Mutual recognition across the EU of TLPT attestation	The RTS should ensure that TLPT attestations issued by a TLPT Authority are mutually recognized across the EU	Already in Article 26(7) of DORA: "Authorities shall provide financial entities with an attestation …in order to allow for mutual recognition of TLPTs between competent authorities"	No change.
Recognition of TLPT test in third countries	The RTS should include provisions allowing for the recognition of TLPT testing conducted outside of the EU. Harmonization with existing national cybersecurity and audit requirements is also needed.	Out of the ESAs' mandate (only within the EU)	No change.
European-wide recognized TLPT provider certification	To facilitate mutual recognition, the RTS should propose the establishment of a European-wide recognized certification for TLPT providers that would be acknowledged by all Member States	Out of the ESAs' mandate.	No change.
Any other comments 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.			
Level of detail in drafting	The appropriateness of the detail level is much closer to an SOP and Framework definition rather than a set of requirements.	/	No change.
Extend implementation timeline	The timeline for implementation is challenging (DORA enters into force 6 months after publication of the RTS), so a proportionate and pragmatic	It is not possible to change Level 1 (DORA) requirements through Level 2 (RTS)	No change.

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
	approach should be ensured in application of the requirements.		
Test environment	Sandbox test environment would be preferable than the live environment	This is established in Article 26 of DORA and connot be changed in the RTS.	No change
Frequency of testing	- There is no clear indicator about how often the TLPT needs to be executed. In the RTS there is only a statement that typically it will be required to execute every 3 years. At a minimum, we recommend that this be 3 years from the end date of the last TLPT, not every 3 calendar years, which we believe would strain the resources of both FEs and TLPT authorities. - Can be cleared up if each test should cover all critical functions, or if not additional test need to be done within the 3 yar frametime to cover all of them? No timelines of TLPT in RTS, it should specify that Significant FE should conduct TLPT within 3 years of DORA entering into force. Any TIBER test performed in 2024 should count as a valid TLPT until end of 2027.	The rules relating to the frequency of TLPTs are established in DORA itself: Article 26(1) provides that "Financial entities, other than entities referred to in Article 16(1), first subparagraph, and other than microenterprises, which are identified in accordance with paragraph 8, third subparagraph, of this Article, shall carry out at least every 3 years advanced testing by means of TLPT. Based on the risk profile of the financial entity and taking into account operational circumstances, the competent authority may, where necessary, request the financial entity to reduce or increase this frequency." There is no mandate for the ESAs to further specify these rules. As of the date of application of DORA i.e. 17 January 2025, FEs will have to	No change.

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
	- The length of TLPTs, including purple teaming and remediation, often extend beyond three years and we strongly support that a TLPT should be conducted from the date of completion from the prior TLPT. - We note paragraph 11 of the consultation paper, which signals that TLPT authorities will have flexibility. We support flexibility in setting the frequency of TLPTs and caution against the rigid enforcement of a 3-year rotation. NCAs should retain the ability to reduce the number of firms in scope beyond what is provided in the RTS, in particular, to opt out branches of larger financial entities in favour of a focus on the most significant EU entity of the group (practical way to reduce the number of firms in scope while achieving the same risk assurance). This approach would make the frequency proposed in the Level 1 text more achievable. - A schedule with the frequency of testing for each FE is needed.	organise TLPTs by default every three years, unless their TLPT authority decides otherwise. To comply with this requirement TLPTs will have to be conducted in accordance wth DORA requirements, as evidenced by the delivery to the FE by the TLPT authority of an attestation referred to in Article 26(7) of DORA.	

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
Increase frequency of tests by external testers	- Every third test, possibly up to 9 years, without external audit is too much. - It is preferable that external testers are used every other test and not every 3 tests.	This comes from Article 26(8) of DORA which requires TLPT to be undertaken by external testers at least every three tests. Frequency of tests to be determined by authority (Article 26(1) of DORA): "*Based on the risk profile of the financial entit and taking into account operational circumstances, the competent authority may, where necessary, request the financial entity tor educe or increase this frequency*".	No change.
TIBER and DORA TLPT	- Maintaining the locally implemented TIBER framework in parallel with DORA/TLPT is in conflict with DORA stated goal of removing market distortions relating to national regulation and supervisory approaches. The duplicate EU regulation should replace the existing TIBER framework to ensure consistent application within the internal market and reduce the cost and complexity of overlapping frameworks that are both EU regulation and locally implemented regulation (TIBER). - TLPT and TIBER-EU should be merged into an identical test method with identical terminology, requirements, procedures etc.	The coexistence of these two frameworks is organised as follows in Recital 1 of the draft RTS: "*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*." TIBER-EU is one framework that can be used to coply with DORA TLPT requirements, but TLPT authorities should assess	No change.

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
TLPTs for FEs belonging to same grou	Are group structure TLPT allowed or only on individual entities? Clarifications on scope also needed It is not clear if a group needs to run one TPLT across the EU/Europe, or if they will have to run separate TPLT's for various individual legal entities among the Group.	Identification of financial entities that are required to perform TLPT is made at the level of the financial entity (although belonging to a group is part of the assessment made by the authority) Tests can be conducted at group level through 'joint tests'.	Clarifications on joint tests and on the process applicable to them.
Timelines for approval by the TLPT Authority	Timelines for all approvals that have to be issued by the TLPT authority are missing throughout the RTS.	To clarify this, a new paragraph (5) has been included in Article 3 of the draft RTS: "*The TLPT authority shall participate to all the phases of the TLPT and shall endeavour to provide feedback, validations or approvals in a period of time adequate to expediently carry out the TLPT*".	New Article 3(5).
Extend possibility to access to information about the TLPT	It is correct that access to information on the TLPT should be on a need-to-know basis. However, the list of groups that have access to parts of the information should be extended. Several processes for organizing and financing a TLPT require members of the financial institution who are not part of the control team or the governing body. An example in most tests is the procurement process, which requires some exceptions to this requirement. This requirement should be amended to allow for	Art 4(2)(a) of the draft RTS: "*access to information pertaining to any planned or on-going TLPT is limited on a need-to-know basis to the control team, the management body, the testers, the TIP and the TLPT authority*." Sharing information beyond the entities listed above is therefore prohibited before and during a TLPT. Once the TLPT is over, non-sensitive information can be shared, also to maximise the learning potential of such test.	No change.

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
	individual exceptions under the supervision of the test managers (or TLPT authority).		
Threat intelligence	Currently the threat intelligence provider has to target each and every critical or important function in the scope of the TLPT. This however contradicts with the threat led approach. If there is not a threat against certain critical functions the threat intelligence provider is forced to make scenarios that cover all critical or important functions of the entity. Suggest to change article 7(2)by removing: 'and shall target each and every critical or important functions in the scope of the TLPT'.	According to DORA Article 26(2) "each TLPT shall cover several or all critical or important functions of a FE", therefore not all critical or important functions have to be in scope of each TLPT of a given FE.	No change needed.
Detection of test activities	How can a detection of testing activities lead to continuation of TLPT without breaking secrecy? What measures should be taken to allow TLPT to continue and how (examples)? How do stakeholders communicate in such a case?	Detection of the testing activities is addressed in Article 10, paragraphs (9) and (10). The conditions of suspension of a test or its continuation through a limited purple teaming exercise have been clarified. The details of communication sto be made in such case will have to be discussed on a case by case basis and cannot be mandated in the RTS. The ESAS note that undetected scenarios can continue in the meantime.	Clarification in Article 10.

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
TLPT Authority	- TLPT should only be involved on the scope of TLPT scenario and after the completion of the tests – otherwise TLPT may be delayed, prolonged and generate significant cost. If TLPT authority must be involved it should respond within specific timelines. It is inappropriate that the TLPT Authorities are tasked "to organise" and "to lead" the tests as we do not find that a TLPT test is an oversight activity. The authorities should review the results of the tests, but they cannot both lead a test and evaluate the results of the test impartially. In addition, the approach is not aligned with Article 26 and Article 27 of the Level 1 text. The draft RTS does not include the obligation for the TLPT authority to set up 'Chinese Walls' (i.e. barriers to information) between the internal TLPT team of the TLPT authority and its regular supervisory teams (e.g. prudential and conduct of business supervision). The outcomes of the TLPT authority should not result in enforcement by the 'regular' supervisory team of the TLPT authority or other NCAs. We suggest adding the requirement of Chinese walls within the TLPT authority to either Article 2 or 3 of the draft RTS. The TIBER-NL	In respect of the absence of hard deadline applicable to TLPT aythorities involvement in the TLPT, it has been clarified that "The TLPT authority shall participate to all the phases of the TLPT and shall endeavour to provide feedback, validations or approvals in a period of time adequate to expediently carry out the TLPT". On the establishment of a separation within the TLPT authority between staff assigned to the supervision of the tested FE and staff assigned to TLPT, Recital (8) strongly encourages TLPT authorities to consider that for the duration of a TLPT, test managers should not conduct supervisory activities on the same financial entity undergoing a TLPT.	New Article 3(5).

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
	framework prescribes that the testing authority gets informed about the preparation and performance of TIBER testing. The authority can only access the documentation at the financial entity's premises, to prevent this very sensitive information is concentrated at one point. The DORA RTS mandates to provide the TPLT authority with this information. There are doubts about the wisdom of this decision.		
Attack paths	this can mean any viable path, not just one used by the testers during an assessment. In some cases, particularly during purple teaming, valid attack paths can be identified from multiple points of testing but are not fully executed during the test.	For the purposes of the RTS, references are only to planned or executed paths.	No change
Annex II - Content of the scope specification document	It is not clear whether the "physical targeting information" consideration at Section 2(g) is directed solely at the physical premises of a financial entity (or whether it includes assets of ICT third-party ICT service providers). The latter should not be within scope of the Threat Intelligence Report, or any aspect of TLPTs, due to the fact that investigation of the physical security of the premises of an ICT third-party provider could endanger the security of that ICT third-party services provider's other customers	Annex III 2(g) only refers to financial entity and does not mention the ICT TPP.	No change

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
	that are not subject to the Regulation. Due to the physical security measures taken over a cloud services provider's data centres, it would be unsafe for any external party to conduct investigations over such premises without providing sufficient notice to the relevant ICT third-party services provider.		
Annex II - Content of the scope specification document	The RTS should only include the list of critical functions that will be tested and not the entire list of the entity's critical functions that constitute confidential information.	The ESAs consider that the scope specificstion document should provide the broadest picture of a FE's critical or important functions. Then the threat intelligence phase will allow narrowing down the list to those critical or important functions that will be effectively included in the scope of the TLPT.	No change.
Annex III - Actionable intelligence	The RTS should be expanded to include credentials that could be located in other repositories, even if those aren't necessarily accessible over the open internet. Open internet is too restrictive.	The ESAs welcome the comment and have deleted the reference to "found on the internet" in paragraph (2)(a).	Change in Annex III.
Time to prepare for a TLPT test	FE should be given enough time to adequately prepare for a TLPT.	TLPT authorities are encouraged to liaise with financial entities required to perform a TLPT as soon as possible after their identification, and financial entities are encouraged to start liaising with TLPT providers (threat intelligence	No change.

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
		pproviders, testers) as soon as possible once they know they are in scope of TLPT.	
Onboarding period	Proposal to include an onboarding period by authorities within the approach to enforcement, ie. FEs can rely on TLPT exercises conducted in 2024 as valid until at least 2027.	This would pose an issue of compliance with the RTS, no attestation could be issued in respect of such tests.	No change.
Shortage of qualified internal and external personnel	Proposal to include provisions that encourage the development and certification of new testers and threat intelligence providers, as well as the fostering of partnerships with academic institutions to ensure a steady pipeline of qualified professionals	This is out of the ESAs' mandate.	No change.
TLPT test on a multi-tenant cloud	TLPT methodology is not suitable for a multi-tenat cloud environment. The RTS should clarify that, where an ICT TPP provider is impacted by the TLPT, that provider should always be informed about the TLPT and, if relevant, be allowed to participate in the test and reduce from 12 to 4 weeks the active red teaming partipation of the test (para. 40 of Section 3)	The RTS provides that staff from an ICT TPP may be included in a control team " where relevant in consideration of the scope of the TLPT".	Change in Article 1
New definition for 'Mixed teams' of	The RTS should include the concept/definition of "mixed team" of internal and external testers for an effective execution of tests as Annex I "Content of	No definition has been introduced, but a clarification is already given in Recital 22 of the	No change.

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
internal and external testers	the project charter" makes a reference to this concept.	RTS that a "mixed team" cannot count as "external tester".	
Clarification of TLPT authority/TCT/ Test manager roles	The RTS should clarify the role/terms of the TLPT CyberTeam and TLPT Authority for consistency. Clarification of "TLPT authority needed for Article 8: In Article 8 sections 5., 6., 8., 9., and 10." The RTS should clarify the difference between "TLPT Authority", "TCT" and "test managers" as these terms seem to basically refer to the same party.	TLPT authority is the authority (or authorities) in charge of some or all TLPT-related matters in relation to a financial entity, and can be national or pan-European (eg. ECB or ESMA). A TCT is a sub-structure that can be set up by an authority to take care of TLPT-related matters and which will typically include test managers, among other staff. Test managers are staff members assigned to actual TLPTs.	Clarification across the RTS
Clarification of definition of blue team / ICT TPP	The FE and TPP have separate blue teams and will not coordinate during a test. We would therefore suggest the following amendment Article 1(3): 'blue team' means the staff of the financial entity and of the financial entity's third-party service providers, that are..." The RTS should clarify the blue team definition and the staff of its third-party services providers to be part of this team (ie. whether it refers to staff within a financial entity's intragroup providers).	Staff of the FE's ICT TPP already included in blue team according to Article 1(3). No distinction based on whether it is an intra-group provider or not.	No change.

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
Clarification of definition of control team /ICT TPP	The definition of the blue team within the RTS infers that CAG's staff and the third-party service provider will be in the same team. The RTS text should be redrafted **to ensure that third party providers are not expected to be part of the control team**. The RTS should clarify the control team definition and the staff of its third-party services providers to be part of this teams (ie. Whether it refers to staff within a financial entity's intragroup providers).	Staff member(s) of the ICT TPP used by the FE may be part of the control team of a given TLPT if this si deemed relevant by the (designated, athe case mey be) FE and the (lead, as the case may be) TLPT authority.	Change in Article 1 and clarification in Article 8(4) of the draft RTS that both the initial composition and any subsequent changes to the control team has to be approved by a TLPT authority.
Clarification of definition of sensitive information / ICT TPP	The definition of "sensitive information" must include the ICT TPP's information where they are required to participate in TLPT.	ICT TPPs being part of the FE's ecosystem, the ESAs consider this is covered by the broad definition of 'sensitive information': "*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*". It does not relate only to FE's information.	No change.
Remediation plan / TPP	It would be appropriate for the cloud services provider to have the opportunity to review the content of a remediation plan. The objective of such a review would purely be to ensure that information	If relevant, staff from the ICT TPP will be included in the control team and will therefore have the opportunity to review the remediation plan.	No change.

Topic	Summary of the comments received *Unless otherwise mentioned, references here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*	Amendments to the proposal
	is not disclosed that could present a security risk to other entities falling outside the scope of the Regulation.		