Official Journal
of the European Union

EN
L series

2025/1190

18.6.2025

COMMISSION DELEGATED REGULATION (EU) 2025/1190

of 13 February 2025

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 the 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 ([1]), 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 threat-led penetration testing (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. The designation of a single public authority in the financial sector that is responsible for TLPT-related matters at national level in accordance with Article 26(9) of Regulation (EU) 2022/2554 should be without prejudice to the competence of competent authorities entrusted at Union level for the supervision of certain financial entities in accordance with Article 46 of that Regulation such as, for instance, the European Central Bank for significant credit institutions which are to be considered competent for TLPT-related matters. Where only some of the tasks related to TLPTs are delegated to another national authority in the financial sector pursuant to Article 26(10) of Regulation (EU) 2022/2554, the competent authority of the financial entity referred to in Article 46 of that Regulation should remain the authority for the TLPT-related tasks that have been not delegated.

(2) Considering the complexity of the TLPT and the risks relating to it, its use should be restricted to those financial entities for which it is justified. Hence, authorities responsible for TLPT matters (TLPT authorities, either at Union or national level) should exclude from the scope of TLPT those financial entities that operate in core financial services subsectors for which a TLPT is not justified. That means that credit institutions, payment and electronic money institutions, central security depositories, central counterparties, trading venues, insurance and reinsurance undertakings, even though they meet the quantitative criteria, could be released from the requirement of TLPT in light of an overall assessment of their ICT risk profile and maturity, impact on the financial sector, and related financial stability concerns.

(3) 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 of 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 whether such financial entities meet those qualitative criteria should aim at identifying financial entities for which TLPT is appropriate by using cross-sector and objective indicators. At the same time, the assessment of whether a financial entity meets those qualitative criteria should limit the entities subject to TLPT to those for which the testing

([1]) OJ L 333, 27.12.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj.

is justified. Whether a financial entity meets those qualitative criteria should also be assessed in the light of new markets development and of the increasing importance of new market participants for the financial sector in the future, including crypto asset service providers authorised in accordance with Article 59 of Regulation (EU) 2023/1114 of the European Parliament and of the Council ([2]).

(4) Financial entities may have the same ICT intra-group service provider or may belong to the same group and rely on the use of shared ICT systems. In that case, it is important that TLPT authorities consider the structure and systemic character or importance for the financial sector of that financial entity 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).

(5) 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 'control team') and a blue team (mirroring the TIBER-EU 'blue team'), and the TLPT authority, in the form of a TLPT cyber team (mirroring the TIBER-EU 'TIBER cyber teams'), a threat intelligence provider, and testers (whereby the testers mirror the TIBER-EU 'red team provider').

(6) 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-EU cyber teams. Hence, the TLPT cyber teams should have test managers that are responsible for overseeing individual TLPTs and for planning and coordinating individual tests. TLPT cyber teams should serve as a single point of contact for test-related communication to internal and external stakeholders, for collecting and processing feedback and lessons learned from previously conducted tests, and for supporting financial entities undergoing TLPT testing.

(7) To mirror the TIBER-EU framework methodology, test managers should have the skills and capabilities necessary to provide advice and to challenge tester proposals. Experience under the TIBER-EU framework has proven that it is 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.

(8) It is important, for consistency with the TIBER-EU framework, that the TLPT authority closely follows the testing in each of its stages. Considering the nature of the testing and the risks associated to it, it is fundamental that the TLPT authority is involved in each specific phase of the testing. 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, influence the effectiveness of the test and, on the other hand, have an impact on the risks associated with the test. The fundamental steps on which a specific involvement of the TLPT authority is necessary include the validation of certain fundamental documentation of the testing, and the selection of threat intelligence providers and testers and risk management measures. The involvement of the TLPT authorities, and in particular for validations, should not result in an excessive burden for those authorities and should therefore be limited to those documentation and decisions that directly affect the conduct of the TLPT. Through the active participation in each phase of the testing, the TLPT authorities may effectively assess compliance of the financial entities with the relevant requirements, which should allow those authorities to issue attestations pursuant to Article 26(7) of Regulation (EU) 2022/2554.

([2]) Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 (OJ L 150, 9.6.2023, p. 40, ELI: http://data.europa.eu/eli/reg/2023/1114/oj).

(9) The secrecy of TLPT is of utmost importance to ensure that the conditions of the testing are realistic. For that reason, testing should be covert, and precautions should be taken to keep the TLPT confidential, including the choice of codenames that should be designed to prevent 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 testing. Staff members of the financial entity outside of the control team should therefore only be made aware of any planned or ongoing TLPT where there are cogent reasons and subject to the prior agreement of the test managers, inter alia to ensure the secrecy of the test in case a blue team member has detected the testing.

(10) As evidenced through the experience gathered in the TIBER-EU framework with respect to the 'control team', the selection of an adequate control team lead is indispensable for the safe conduct of TLPT. The control team lead should have the necessary mandate within the financial entity to guide all the aspects of the testing, without compromising its confidentiality. For the same reason, members of the control team should have a deep knowledge of the financial entity, of the control team lead's job role and strategic positioning, should have the required seniority and should have access to the management board. To reduce the risk of compromising the TLPT, the control team should be as small as possible.

(11) There are inherent elements of risks associated with TLPT as critical functions are tested in a 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. Those risks highlight the need for robust risk management measures. To ensure that the TLPT is conducted in a controlled manner all along the testing, it is very important that financial entities are at all points aware of the particular risks that arise in a TLPT and that those risk are mitigated. 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 about the TLPT risk management measures, or, in particular cases the approval of those risk management measures by the financial entity's management body itself, may be appropriate. To be able to deliver effective and most qualified professional services and to reduce those risks, it is also essential that the testers and threat intelligence providers (together, the TLPT providers) have the highest level of skills, expertise, and an appropriate experience in threat intelligence and TLPT in the financial services industry.

(12) Conventional penetration tests provide a detailed and useful assessment of technical and configuration vulnerabilities often of a single system or environment in isolation, but unlike intelligence led red team test, 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 of the TLPT providers, financial entities should therefore ensure that those providers have the requisite skills to perform intelligence-led red team tests, and not only penetration tests. It is therefore necessary to lay down comprehensive criteria for testers, both internal and external, and threat intelligence providers, always external. Where the TLPT providers belong to the same company, the staff assigned to a TLPT should be adequately separated.

(13) There may be exceptional circumstances where financial entities are unable to contract TLPT providers that meet the comprehensive criteria. Financial entities, upon evidencing the unavailability of such threat intelligence providers, should therefore be allowed to engage persons who do not satisfy all comprehensive criteria, provided that they properly mitigate any resultant additional risks and that the TLPT authority assesses all those criteria.

(14) Where 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, namely that it should be in charge of providing all necessary documentation to the lead TLPT authority and of 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 should remain unaffected during the pooled test. The same principle should apply for joint TLPTs.

(15) As evidenced by the experience of the implementation of the TIBER-EU framework, holding in-person or virtual meetings including all stakeholders concerned (financial entities, authorities, testers and threat intelligence providers) is the most efficient way to ensure the appropriate conduct of the testing. In-person and virtual meetings should therefore 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 replaying testers and blue team actions, purple teaming and to exchange feedback on the TLPT.

(16) To ensure the smooth performance of the TLPT, the TLPT authority should clearly present to the financial entity its expectations with respect to the testing. In that respect, the test managers should ensure that an appropriate flow of information is established with the control team within the financial entity, and with the TLPT providers.

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

(18) 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, 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. To ensure that the threat intelligence provider considers the relevant threats for the financial entity, the testers, the control team, and the test managers should provide feedback the draft threat intelligence report. If it is available, the threat intelligence provider may use a generic threat landscape provided by the TLPT authority for the financial sector of a Member State as a baseline for the national threat landscape. Based on the TIBER-EU framework application, the threat intelligence gathering process typically lasts approximately 4 weeks.

(19) To enable the testers to gain insight and further review the scope specification document and targeted threat intelligence report to finalise the red team testing plan, it is essential that, prior to the red team testing phase of the TLPT, the testers receive from the threat intelligence provider detailed explanations on the targeted threat intelligence report and analysis of possible threat scenarios.

(20) To enable testers to conduct a realistic and comprehensive testing in which all attack phases are executed and flags are reached, sufficient time should be allocated to the active red team testing phase. On the basis of the experience gathered with the TIBER-EU framework, the time allocated should be at least 12 weeks and should 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 contain, 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 compromised systems to further vulnerable or high value ones), and actions on target (i.e. gaining further access to compromised 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 categorised in information and access leg-ups and may consist of the provision of access to ICT systems 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, if necessary to allow for the continuation of the TLPT as a last resort in exceptional circumstances and once all alternative options have been exhausted, a collaborative testing activity that involves both the testers and the blue team, should be used. In the context of such 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, 'war gaming', which allows for more complex scenarios to test strategic decision-making, or 'collaborative proof-of-concept' which enables 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 to learn from the testing experience in collaboration with the testers. For that 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 maximise the learning experience. Methods that may be used for purple teaming in the closure phase should 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, the parties concerned should provide feedback to each other on the overall process, and in particular identify which activities progressed well or could have been improved, and which aspects of the TLPT process worked well or could be improved.

(26) The competent authorities referred to in Article 46 of Regulation (EU) 2022/2554 and TLPT authorities, where different, should cooperate to incorporate advanced testing by means of TLPT into the existing supervisory processes. In that respect and to share the correct understanding of the TLPT findings and of how they should be interpreted, it is appropriate that, in particular 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.

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

(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 ([3]), 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 ([4]), 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 ([5]).

(30) The European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 of the European Parliament and of the Council ([6]) and delivered an opinion on 20 August 2024,

HAS ADOPTED THIS REGULATION:

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 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) 'red team' means the testers, internal or external, contracted for, or assigned to, a TLPT;

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

([3]) 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, ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

([4]) 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, ELI: http://data.europa.eu/eli/reg/2010/1094/oj).

([5]) 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, ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

([6]) Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

(7) 'TLPT authority' means any of the following:

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

(b) 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;

(c) any of the competent authorities referred to in Article 46 of Regulation (EU) 2022/2554;

(8) 'TLPT Cyber Team' or 'TCT' means the staff within the TLPT authorities that is responsible for TLPT-related matters;

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

(10) 'threat intelligence provider' means the experts, contracted by the financial entity for each TLPT, and 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;

(11) 'TLPT providers' means testers and threat intelligence providers;

(12) 'leg-up' means the assistance or information provided by the control team to the testers to enable 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;

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

(14) '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;

(15) '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, or personal data, that can directly or indirectly harm the financial entity and its ecosystem would it fall in the hands of malicious actors;

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

(17) 'host Member State' means the host Member State in accordance with the Union sectoral law applicable to each financial entity;

(18) 'joint TLPT' means a TLPT, other than a pooled TLPT as 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 sharing ICT systems.

Article 2

Identification of financial entities required to perform TLPT

1. TLPT authorities shall assess whether any financial entity is required to perform TLPT, taking into account the impact of those financial entities, their systemic character and their ICT risk profile, 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 on the basis of whether the financial entity provides financial services in one or more Member States and by comparing the activities of the financial entity to those of other financial entities providing similar services;

(ii) the extent and nature of the interconnectedness of the financial entity with other financial entities in the financial sector in one or more Member States;

(iii) the criticality or importance of the services that the financial entity provides to the financial sector;

(iv) the substitutability of the services that the financial entity provides;

(v) the complexity of the business model of the financial entity and the related services and processes;

(vi) whether the financial entity is part of a group of systemic character at Union or national level in the financial sector and sharing 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, and the quantity and type of contractual arrangements with ICT third-party service providers or ICT intra-group service providers;

(vi) the 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:

(1) monitor the financial entity's ICT infrastructure on a permanent basis;

(2) detect ICT-related events in real time;

(3) analyse the events referred to in point (2);

(4) respond to the events referred to in point (2) 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 that shares ICT systems.

For the purposes of point (a)(i), the TLPT authority shall, where possible, consider:

(a) the market share position of the financial entity at Union and national level;

(b) the range of activities offered by the financial entity;

(c) the market share of the services provided by the financial entity or of the activities undertaken at Union and national level.

For the purposes of point (a)(v), the TLPT authority shall, where possible, consider:

(a) whether the financial entity operates more than one business model;

(b) the interconnectedness of different business processes and the related services.

2. TLPT authorities shall require all of the following financial entities to perform TLPT, unless the assessment referred to in paragraph 1 in respect of a financial entity indicates that its impact, the financial stability concerns relating to that financial entity, or its ICT risk profile, does not justify the performance of a TLPT:

(a) credit institutions that meet any of the following conditions:

(i) they have been 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 ([7]);

(ii) they have been identified as other systemically important institutions (O-SIIs) in accordance with Article 131 of Directive 2013/36/EU;

(iii) they are part of a G-SIIs or O-SIIs;

([7]) 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, ELI: http://data.europa.eu/eli/dir/2013/36/oj).

(b) payment institutions that exceeded in each of the 2 calendar years preceding the assessment by the TLPT authority EUR 150 billion of total value of payment transactions as defined in Article 4, point (5), of Directive (EU) 2015/2366 of the European Parliament and of the Council ([8]);

(c) electronic money institutions that exceeded in each of the 2 calendar years preceding the assessment by the TLPT authority either EUR 150 billion of total value of payment transactions as defined in Article 4, point (5), 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 any of the following criteria:

(i) the trading venue has the highest market share in terms of turnover at national level in each of the 2 calendar years preceding the assessment by the TLPT authority in any of the following:

(1) transferable securities as defined in Article 4(1), point (44)(a), of Directive 2014/65/EU of the European Parliament and of the Council ([9]);

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

(3) derivatives as defined in Article 2(1), point (29), of Regulation (EU) No 600/2014 of the European Parliament and of the Council ([10]);

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

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

(ii) the trading venue has a market share in terms of turnover at Union level that exceeds 5 % in each of the 2 calendar years preceding the assessment by the TLPT authority in any of the following:

(1) shares in companies and other securities equivalent to shares in companies, partnerships or other entities, and depositary receipts in respect of shares;

(2) bonds or other forms of securitised debt, including depositary receipts in respect of such securities;

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

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

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

([8]) 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, ELI: http://data.europa.eu/eli/dir/2015/2366/oj).

([9]) 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 (OJ L 173, 12.6.2014, p. 349, ELI: http://data.europa.eu/eli/dir/2014/65/oj).

([10]) 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, ELI: http://data.europa.eu/eli/reg/2014/600/oj).

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

(i) they have a gross written premium (GWP) that exceeds EUR 1 500 000 000;

(ii) they have technical provisions that exceed EUR 10 000 000 000;

(iii) insurance undertakings that pursue only life activities or that pursue both life and non-life activities and that have total assets that exceed 3,5 % of the sum of the total assets valuated in accordance with Article 75 of Directive 2009/138/EC of the European Parliament and of the Council ([11]) of the insurance and reinsurance undertakings established in the Member State.

For the purposes of (f)(ii), where the trading venue is part of a group sharing 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.

For the purposes of point (g), TLPT authorities shall identify a subset of all insurance and reinsurance undertakings by applying the criteria laid down in points (g)(i), (ii), and (iii). Insurance and reinsurance undertakings included in that subset shall be required to perform TLPT where they also meet any of the following criteria:

(a) gross written premium (GWP) that exceeds EUR 3 000 000 000;

(b) technical provisions that exceed EUR 30 000 000 000;

(c) total assets that exceed 10 % of the sum of the total assets valuated in accordance with Article 75 of Directive 2009/138/EC of the insurance and reinsurance undertakings established in the Member State.

3. Where more than one financial entity belonging to the same group and sharing ICT systems, or where more than one financial entity using the same ICT intra-group service provider, meet the criteria set out in paragraph 2, the TLPT authorities of those financial entities shall, in accordance with Article 16(2), decide whether the requirement to perform TLPT on an individual basis is relevant for those financial entities.

Where the TLPT authority of the parent undertaking of a group of financial entities referred to in the first subparagraph is different from the TLPT authorities of the financial entities of the group, that authority shall be consulted by the TLPT authorities of the financial entities belonging to that group on whether it is appropriate to perform TLPT on an individual basis.

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 be composed of test managers that are assigned to oversee an individual TLPT.

2. For each test, the TLPT authority shall designate a test manager and at least one alternate.

3. The test managers shall monitor whether, and ensure that, the requirements laid down in this Regulation are complied with.

([11]) 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) (OJ L 335, 17.12.2009, p. 1, ELI: http://data.europa.eu/eli/dir/2009/138/oj).

4. The test manager shall communicate the contact details of the TCT to the financial entity through the notification referred to in Article 9(1).

5. The TLPT authority shall participate to all the phases of the TLPT.

Article 4

Organisational arrangements for financial entities

1. Financial entities shall appoint a control team lead which 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 to ensure 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; in case of escalation of the resulting incident response, where needed, the control team contains such escalation;

(d) arrangements relating to the secrecy of the TLPT, applicable to staff of the financial entity, to the staff of the ICT third party service providers concerned, 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 9, the control team shall assess the risks associated with the testing of live production systems of critical or important functions of the financial entity, including potential impacts on:

(a) the financial sector;

(b) the financial stability at Union or national level.

The control team shall review those impacts throughout the testing.

2. For the purposes of the risk assessment and management, the control team shall take into account at least the following types of risks related to:

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

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

(c) crisis and incident escalation;

(d) the active red team phase, including risks related to the interruption of critical activities and the corruption of data due to the activities of the testers, and its potential impacts on third parties;

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

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

Article 6

Risk management for pooled or 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 16(3), point (b), of this Regulation, or the financial entity designated in accordance with Article 26(4) of Regulation (EU) 2022/2554, shall assess the risks relating to the involvement in the TLPT of multiple financial entities. The control teams of the involved financial entities shall cooperate with the control team of the designated financial entity to identify potential joint risks.

Article 7

Selection of TLPT providers

1. The control team shall take measures to manage the risks relating to the TLPT and shall in particular ensure that, for each TLPT:

(a) the threat intelligence provider and external testers provide the control team with a detailed *curriculum vitae* and copies of certifications that, according to recognised market standards, are appropriate for the performance of their activities;

(b) the threat intelligence provider and external tester are duly and fully covered by proper 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:

(i) is composed of at least a manager with at least 5 years' experience in threat intelligence and at least one additional member with at least 2 years' experience in threat intelligence;

(ii) display a broad range and appropriate level of professional knowledge and skills, including:

(1) intelligence gathering tactics, techniques and procedures;

(2) geopolitical, technical and sectorial knowledge;

(3) adequate communication skills to clearly present and report on the result of the engagement;

(iii) has a combined participation in at least three previous assignments in threat intelligence in the context of penetration testing and red team testing;

(iv) does 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) is separated from and not reporting to staff of the same TLPT provider providing external testers for the same TLPT;

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

(i) is composed of at least a manager, with at least 5 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 2 years;

(ii) displays 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) has a combined participation in at least five previous assignments related to penetration testing and red team testing;

(iv) is not employed by, nor provides services to, a threat intelligence provider that simultaneously performs blue team tasks for either a financial entity, an ICT third-party service provider, or an ICT intra-group service provider that is involved in the TLPT;

(v) is separated from any staff of the same TLPT provider that simultaneously provides threat-intelligence services for the same TLPT;

(g) the testers and the threat intelligence provider 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 other data collected during testing;

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

(i) command and control deactivation;

(ii) scope and date kill switches;

(iii) removal of backdoors and other malware;

(iv) potential breach notification;

(v) procedures for future back-up restoration which may concern malware or tools installed during the test;

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

(i) testers and the threat intelligence provider do not perform, or participate in, any of 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.

2. The control team shall keep record of the documentation provided by the testers and the threat intelligence providers to evidence compliance with paragraph 1, points (a) to (f).

In exceptional circumstances, financial entities may contract external testers and threat intelligence providers that do not meet one or more of the requirements set out in paragraph 1, points (a) to (f), provided that those financial entities adopt measures that are appropriate to mitigate the risks relating to the lack of compliance with such points and record those measures.

Article 8

Specificities for pooled or joint TLPTs

1. Unless otherwise decided by the lead TLPT authority, where several financial entities, identified in accordance with Article 16(2) or (4), are involved in a pooled or joint TLPT, each financial entity shall follow each of the steps set out in Articles 9 to 15.

2. Unless otherwise provided in this Regulation, where several TLPT authorities are involved in a joint TLPT or in a pooled TLPT, as referred to in Article 16(3) or 16(5), references in Articles 9 to 15 to the 'TLPT authority' shall be understood as a reference to the lead TLPT authority for such pooled or joint TLPT.

Article 9

Preparation phase

1. A financial entity identified pursuant to Article 26, paragraph 8, third subparagraph of Regulation (EU) 2022/2554 shall initiate a TLPT following a notification from the TLPT authority that a TLPT is to be carried out.

2. A financial entity shall, within 3 months from having received the notification referred to in paragraph 1, submit to the test managers all of the following TLPT initiation information:

(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 the intended use of internal or external testers or both, where relevant as detailed in Article 15;

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

(e) the code name for the TLPT.

3. Where the information referred to in paragraph 2, points (a) to (e), is complete and ensures the suitability and effective performance of the TLPT, the TLPT authority shall validate the TLPT initiation information of the financial entity and notify the financial entity thereof.

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

(a) specifying 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 this Regulation;

(e) selecting the threat intelligence provider for the TLPT;

(f) selecting the external testers, the internal testers or both;

(g) preparing the scope specification document.

5. 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 4, the TLPT authority shall validate the control team and notify the control team lead thereof.

6. The financial entity shall submit a scope specification document containing all information set out in Annex II to the test managers within 6 months from the receipt of the notification from the TLPT authority referred to in paragraph 1. The management body of the financial entity shall approve the scope specification document.

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

(a) the criticality or importance of the function and its possible impact on the financial sector and on financial stability at Union and national 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.

8. The control team shall share the TLPT initiation information and the scope specification document with the testers and threat intelligence providers once those are contracted. The control team shall inform the testers and threat intelligence providers about the testing process to be followed.

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

10. 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 is of the opinion that they do not adequately address the risks of the TLPT.

11. The control team shall assess the compliance of threat intelligence providers and testers they consider involving in the TLPT with the requirements laid down in Article 27 of Regulation (EU) 2022/2554 and with Article 7(1) of this Regulation, and document the outcome of that assessment. The control team shall select threat intelligence providers in accordance with that assessment and with its risk management practices. Prior to contracting the selected threat intelligence providers and external testers, the control team shall provide to the test managers evidence of compliance of those threat intelligence providers and testers with the requirements laid down in Article 27 of Regulation (EU) 2022/2554 and with Article 7(1) of this Regulation. The control team shall not proceed with contracting the selected threat intelligence providers and external testers where the TLPT authority is of the opinion that the selected threat intelligence providers and external testers do not comply with the requirements laid down in Article 27 of Regulation (EU) 2022/2554, or with the requirements laid down in Article 7(1) of this Regulation or with additional requirements stemming from national security legislations in accordance with Union law, or where the financial entity does not comply with Article 7(2), first subparagraph, of this Regulation, or where the circumstances referred to in Article 7(2), second subparagraph, of this Regulation are not met.

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

Article 10

Testing phase: threat intelligence

1. Following the 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. Where a generic threat landscape has been provided by the TLPT authority for the financial sector of a Member State, the threat intelligence provider may use that landscape as a baseline for the national threat landscape. 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 contextualised 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 requisite 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 critical or important function 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 testing, 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 in accordance with paragraphs 3 and 4. The threat intelligence report shall contain 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 ensures the performance of an effective TLPT, the TLPT authority shall approve the targeted threat intelligence report and inform the control team lead thereof.

Article 11

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 contain 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. Where the red team test plan is complete and ensures the performance of an effective TLPT, the control team and the TLPT authority shall approve the red team test plan and the TLPT shall inform the control team lead thereof.

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 12 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. Subject to ensuring that the red team test plan remains complete and allows for the performance of an effective TLPT, the control team lead and the test managers shall approve any changes to the red team test plan subsequent to its approval, including to the timeline, scope, target systems or flags.

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 the 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, where 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 12-week minimum duration of the active red team testing phase referred to in paragraph 5.

Article 12

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 4 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. The control team shall provide the red team test report to the blue team and test managers without undue delay.

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

4. Upon receipt of the red team test report, and no later than 10 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. The control team shall provide the blue team test report to the testers and the test managers without undue delay.

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

5. No later than 10 weeks after the end of the active red team testing phase, the blue team and the testers shall replay 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 Annexes V and VI, the financial entity shall within 8 weeks submit the report summarising the relevant findings of the TLPT to the TLPT authority, as 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 shall not contain sensitive information.

Article 13

Remediation plan

1. Within 8 weeks from the notification referred to in Article 12(7) of this Regulation, the financial entity shall provide the remediation plans and the documentation 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, measures 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.

Article 14

Attestation

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

2. Where several TLPT authorities have been involved in a TLPT, the lead TLPT authority shall provide the attestation referred to in Article 26(7) of Regulation (EU) 2022/2554 to the tested financial entities.

Article 15

Use of internal testers

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

(a) the establishment and implementation of a policy for the management of internal testers in a TLPT;

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

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

The policy referred to in point (a) shall:

(a) contain criteria to assess suitability, competence, potential conflicts of interest of the internal testers and specify management responsibilities in the testing process;

(b) be documented and periodically reviewed;

(c) provide that the internal testing team includes a test lead, and at least two additional members;

(d) 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;

(e) include provisions on training on how to perform penetration testing and red team testing of the internal testers.

2. Where a TLPT authority approves the use of internal testers in accordance with Article 27(2), point (a), of Regulation (EU) 2022/2554, the TLPT authority shall consider the requirements laid down in Article 7(1) of this Regulation.

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

(a) the test initiation information referred to in Article 9;

(b) the red team test report referred to in Article 12(2);

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

4. Testers employed by an ICT intra-group service provider shall be considered as internal testers of the financial entity.

Article 16

Cooperation and mutual recognition

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 in accordance with point (a) of the decision to carry out a TLPT test on the financial entity;

(c) unless otherwise agreed by the TLPT authorities, the TLPT authority of the financial entity shall lead the TLPT.

The TLPT authorities of the host Member States may, within 20 working days from the receipt of the information on a future conduct of a TLPT, either express their interest in following the TLPT as observers or assign a test manager to participate in 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 shares ICT systems with 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 sharing 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 testing 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 of 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 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, those 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 that Regulation.

Article 17

Entry into force

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, 13 February 2025.

For the Commission
The President
Ursula VON DER LEYEN

ANNEX I

Content of the project charter (Article 9(2)(a))

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 9(2), point (d), and Article 9(4) 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 9	yyyy-mm-dd
(2) Testing Phase, in accordance with Articles 10 and 11	yyyy-mm-dd
(3) Closure Phase, in accordance with Article 12	yyyy-mm-dd
(4) Remediation plan in accordance with Article 13	yyyy-mm-dd

ANNEX II

Content of the scope specification document (Article 9(6))

1. The scope specification document shall contain 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 that 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 or availability is covered by each flag.

ANNEX III

Content of the targeted threat intelligence report (Article 10(5))

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

1. The 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. The overall assessment of what concrete actionable intelligence can be found about the financial entity, including:
   (a) the employee usernames and passwords;
   (b) the look-alike domains which can be mistaken for official domains of the financial entity;
   (c) technical reconnaissance: vulnerable or exploitable software, systems and technologies;
   (d) information posted by employees on the internet, 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) the geopolitical environment;
   (b) the 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, a description of the non-threat-led scenario referred to in Article 10(4).

ANNEX IV

Content of the red team test plan (Article 11(1))

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

(a) communication channels and procedures;

(b) the tactics, techniques and procedures allowed and not-allowed for use in the attack, including ethical boundaries for social engineering;

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

(d) a description for each scenario, including:

  (i) the simulated threat actor;

  (ii) their intent, motivation and goals;

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

  (iv) the targeted confidentiality, integrity, availability and authenticity aspects;

  (v) flags;

(e) 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;

(f) the 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);

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

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

ANNEX V

Content of the red team test report (Article 12(2))

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

(a) information on the performed attack, including:

  (i) 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;

  (ii) summary of each scenario;

  (iii) flags reached and not reached;

  (iv) attack paths followed successfully and unsuccessfully;

  (v) tactics, techniques and procedures used successfully and unsuccessfully;

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

  (vii) 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:

  (i) vulnerability and other finding description including their criticality;

  (ii) root cause analysis of successful attacks;

  (iii) recommendations for remediation including indication of the remediation priority.

ANNEX VI

Content of the blue team test report (Article 12(4))

The blue team test report shall contain information on at least all 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 contain information on at least all 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 referred to in Article 26(7) of Regulation (EU) 2022/2554

The attestation shall contain at least all of the following information:

(a) on the performed TLPT:

  (i) the starting and end dates of the TLPT;

  (ii) the critical or important functions in scope of the test;

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

  (iv) where relevant, other financial entities that were involved in the TLPT;

  (v) where relevant, the ICT third-party services providers that participated in the TLPT;

  (vi) in respect of testers:

    1. whether internal testers were used;

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

  (vii) 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.