EUROPEAN
COMMISSION

Brussels, 13.2.2025
C(2025) 885 final

ANNEXES 1 to 8

ANNEXES

to the

COMMISSION DELEGATED REGULATION (EU) …/...

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.

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.