Council of the European Union

Brussels, 23 November 2026
(OR. en)

6302/25
COR 3

EF 34
ECOFIN 162
DELACT 10
ECB

COVER NOTE

From:	Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director
To:	Ms Thérèse BLANCHET, Secretary-General of the Council of the European Union
No. Cion doc.:	C(2026) 8403 final
Subject:	CORRIGENDUM to 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 (Official Journal of the European Union L, 2025/1190, 18 June 2025)

Delegations will find attached document C(2026) 8403 final.

Encl.: C(2026) 8403 final

EUROPEAN
COMMISSION

Brussels, 18.11.2026
C(2026) 8403 final

CORRIGENDUM

to 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

(Official Journal of the European Union L, 2025/1190, 18 June 2025)

CORRIGENDUM

to 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

(Official Journal of the European Union L, 2025/1190, 18 June 2025)

On page 1, Recital 2:

*for***:** '(2) [...] 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.'

read: '(2) […] That means that credit institutions, payment and electronic money institutions, central securities 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.'

On page 1, Recital 3:

for: '(3) […] 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).'

read: '(3) […] 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).'

On page 3, Recital 10:

for: '(10) […] 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. […]'

read: '(10) […] 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 body. […]'

On page 3, Recital 11:

for: '(11) […] 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. […]'

read: '(11) […] 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 risks are mitigated. […]'

On page 3, Recital 12:

for: '(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. […]'

read: '(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. […]'

On page 3, Recital 14:

for: '(14) […] 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. […]'

read: '(14) […] Notwithstanding the role of the designated financial entity, the obligations of each financial entity participating in the pooled TLPT process should remain unaffected during the pooled test. […]'

On page 4, Recital 15:

for: '(15) […] 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.'

read: '(15) […] 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 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.'

On page 4, Recital 18:

for: '(18) […] 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. […]'

read: '(18) […] 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 on the draft threat intelligence report. […]'

On page 5, Recital 23:

for: '(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. […]'

read: '(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. […]'

On page 7, Article 1, point (8):

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

read: '(8) TLPT Cyber Team' or 'TCT' means the staff within the TLPT authorities who are responsible for TLPT-related matters;'

On page 8, Article 2, paragraph 2, point (a), point (iii):

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

read: '(iii) they are part of a G-SII or O-SII;'

On page 9, Article 2, paragraph 2, point (f), point (ii), points (1) and (2):

for: '(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;'

read: '(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;

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

On page 13, Article 7, paragraph 1, point (f), point (iv):

for: '(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;'

read: '(iv) is not employed by, nor provides services to, a 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;'

On page 29, In Annex VIII, point (a)(vi)(2):

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

read: ‘2. whether Article 7(2)**,** second subparagraph, was used by the financial entity;