Rat der
Europäischen Union

Brüssel, den 11. Juni 2025
(OR. en)

6302/25
COR 2

EF 34
ECOFIN 162
DELACT 10
ECB

ÜBERMITTLUNGSVERMERK

Absender:	Frau Martine DEPREZ, Direktorin, im Auftrag der Generalsekretärin der Europäischen Kommission
Eingangsdatum:	10. Juni 2025
Empfänger:	Frau Thérèse BLANCHET, Generalsekretärin des Rates der Europäischen Union
Nr. Komm.dok.:	C(2025) 3781 final
Betr.:	BERICHTIGUNG vom 6.6.2025 der Delegierten Verordnung (EU) der Kommission vom 13. Februar 2025 zur Ergänzung der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards zur Festlegung der Kriterien für die Bestimmung der Finanzunternehmen, die zur Durchführung von bedrohungsorientierten Penetrationstests verpflichtet sind, der Anforderungen und Standards für den Einsatz interner Tester, der Anforderungen hinsichtlich des Testumfangs, der Testmethodik und des Testkonzepts für jede einzelne Phase des Testverfahrens sowie der Ergebnisse, des Abschlusses und der Behebungsphasen der Tests sowie der Art der aufsichtlichen und sonstigen relevanten Zusammenarbeit, die für die Umsetzung von bedrohungsorientierten Penetrationstests und die Erleichterung der gegenseitigen Anerkennung dieser Tests erforderlich ist (*C(2025) 885 final*)

Die Delegationen erhalten in der Anlage das Dokument C(2025) 3781 final.

Anl.: C(2025) 3781 final

EUROPÄISCHE
KOMMISSION

Brüssel, den 6.6.2025
C(2025) 3781 final

BERICHTIGUNG

vom 6.6.2025

der Delegierten Verordnung (EU) der Kommission vom 13. Februar 2025 zur Ergänzung der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards zur Festlegung der Kriterien für die Bestimmung der Finanzunternehmen, die zur Durchführung von bedrohungsorientierten Penetrationstests verpflichtet sind, der Anforderungen und Standards für den Einsatz interner Tester, der Anforderungen hinsichtlich des Testumfangs, der Testmethodik und des Testkonzepts für jede einzelne Phase des Testverfahrens sowie der Ergebnisse, des Abschlusses und der Behebungsphasen der Tests sowie der Art der aufsichtlichen und sonstigen relevanten Zusammenarbeit, die für die Umsetzung von bedrohungsorientierten Penetrationstests und die Erleichterung der gegenseitigen Anerkennung dieser Tests erforderlich ist

(*C(2025) 885 final*)

BERICHTIGUNG

der Delegierten Verordnung (EU) der Kommission vom 13. Februar 2025 zur Ergänzung der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards zur Festlegung der Kriterien für die Bestimmung der Finanzunternehmen, die zur Durchführung von bedrohungsorientierten Penetrationstests verpflichtet sind, der Anforderungen und Standards für den Einsatz interner Tester, der Anforderungen hinsichtlich des Testumfangs, der Testmethodik und des Testkonzepts für jede einzelne Phase des Testverfahrens sowie der Ergebnisse, des Abschlusses und der Behebungsphasen der Tests sowie der Art der aufsichtlichen und sonstigen relevanten Zusammenarbeit, die für die Umsetzung von bedrohungsorientierten Penetrationstests und die Erleichterung der gegenseitigen Anerkennung dieser Tests erforderlich ist

(*C(2025) 885 final*)

Erwägungsgrund 5:

Anstatt: „(5) Um dem TIBER-EU-Rahmen Rechnung zu tragen, muss die Testmethodik die Einbeziehung der folgenden Hauptbeteiligten vorsehen: das Finanzunternehmen mit einem Kontrollteam (das dem „White Team“ im Rahmen von TIBER-EU entspricht) und einem Blue Team (das dem „Blue Team“ im Rahmen von TIBER-EU entspricht) und die TLPT-Behörde in Form eines TLPT-Cyberteams (das dem „TIBER-Cyberteam“ im Rahmen von TIBER-EU entspricht), ein Anbieter von Bedrohungsanalysen und Tester (wobei die Tester dem „Red-Team-Anbieter“ im Rahmen von TIBER-EU entsprechen).“

muss es heißen: „(5) Um dem TIBER-EU-Rahmen Rechnung zu tragen, muss die Testmethodik die Einbeziehung der folgenden Hauptbeteiligten vorsehen: das Finanzunternehmen mit einem Kontrollteam (das dem „Kontrollteam“ im Rahmen von TIBER-EU entspricht) und einem Blue Team (das dem „Blue Team“ im Rahmen von TIBER-EU entspricht) und die TLPT-Behörde in Form eines TLPT-Cyberteams (das dem „TIBER-Cyberteam“ im Rahmen von TIBER-EU entspricht), ein Anbieter von Bedrohungsanalysen und Tester (wobei die Tester dem „Red-Team-Anbieter“ im Rahmen von TIBER-EU entsprechen).“

Erwägungsgrund 10:

Anstatt: „(10) Wie die im Rahmen des TIBER-EU-Rahmens gewonnenen Erkenntnisse in Bezug auf das „White Team“ gezeigt haben, ist die Auswahl eines geeigneten Leiters für das Kontrollteam unerlässlich für die sichere Durchführung des TLPT. Der Leiter des Kontrollteams sollte innerhalb des Finanzunternehmens über das erforderliche Mandat verfügen, um über alle Aspekte des Tests zu entscheiden, ohne dessen Vertraulichkeit zu gefährden. Aus demselben Grund sollten die Mitglieder des Kontrollteams über weitreichende Kenntnisse des Finanzunternehmens, der Rolle und der strategischen Positionierung des Leiters des Kontrollteams verfügen, die erforderliche hierarchische Position und Zugang zur Geschäftsleitung haben. Um das Risiko einer Gefährdung des TLPT zu verringern, sollte das Kontrollteam so klein wie möglich sein.“

muss es heißen: „(10) Wie die im Rahmen des TIBER-EU-Rahmens gewonnenen Erkenntnisse in Bezug auf das „Kontrollteam“ gezeigt haben, ist die Auswahl eines

geeigneten Leiters für das Kontrollteam unerlässlich für die sichere Durchführung des TLPT. Der Leiter des Kontrollteams sollte innerhalb des Finanzunternehmens über das erforderliche Mandat verfügen, um über alle Aspekte des Tests zu entscheiden, ohne dessen Vertraulichkeit zu gefährden. Aus demselben Grund sollten die Mitglieder des Kontrollteams über weitreichende Kenntnisse des Finanzunternehmens, der Rolle und der strategischen Positionierung des Leiters des Kontrollteams verfügen, die erforderliche hierarchische Position und Zugang zur Geschäftsleitung haben. Um das Risiko einer Gefährdung des TLPT zu verringern, sollte das Kontrollteam so klein wie möglich sein."

Artikel 2 Absatz 3 Unterabsatz 1:

Anstatt: „(3) Erfüllen mehrere Finanzunternehmen, die derselben Gruppe angehören und IKT-Systeme gemeinsam nutzen, oder mehrere Finanzunternehmen, die denselben gruppeninternen IKT-Dienstleister in Anspruch nehmen, die in Absatz 2 genannten Kriterien, so entscheiden die für diese Finanzunternehmen zuständigen TLPT-Behörden gemäß Artikel 14 Absatz 2, ob die Pflicht zur Durchführung von TLPT auf Einzelbasis für diese Finanzunternehmen relevant ist."

muss es heißen: „(3) Erfüllen mehrere Finanzunternehmen, die derselben Gruppe angehören und IKT-Systeme gemeinsam nutzen, oder mehrere Finanzunternehmen, die denselben gruppeninternen IKT-Dienstleister in Anspruch nehmen, die in Absatz 2 genannten Kriterien, so entscheiden die für diese Finanzunternehmen zuständigen TLPT-Behörden gemäß Artikel 16 Absatz 2, ob die Pflicht zur Durchführung von TLPT auf Einzelbasis für diese Finanzunternehmen relevant ist."

Artikel 5 Absatz 1, einleitender Teil:

Anstatt: „(1) Während der Vorbereitungsphase gemäß Artikel 8 bewertet das Kontrollteam die Risiken im Zusammenhang mit Tests der Live-Produktionssysteme kritischer oder wichtiger Funktionen des Finanzunternehmens, einschließlich möglicher Auswirkungen auf"

muss es heißen: „(1) Während der Vorbereitungsphase gemäß Artikel 9 bewertet das Kontrollteam die Risiken im Zusammenhang mit Tests der Live-Produktionssysteme kritischer oder wichtiger Funktionen des Finanzunternehmens, einschließlich möglicher Auswirkungen auf"

Artikel 6 Absatz 2:

Anstatt: „(2) Das Kontrollteam des gemäß Artikel 14 Absatz 3 Buchstabe b dieser Verordnung benannten Finanzunternehmens oder das gemäß Artikel 26 Absatz 4 der Verordnung (EU) 2022/2554 benannte Finanzunternehmen bewertet die Risiken in Verbindung mit der Beteiligung mehrerer Finanzunternehmen an dem TLPT. Die Kontrollteams der beteiligten Finanzunternehmen arbeiten mit dem Kontrollteam des benannten Finanzunternehmens zusammen, um potenzielle gemeinsame Risiken zu ermitteln."

muss es heißen: „(2) Das Kontrollteam des gemäß Artikel 16 Absatz 3 Buchstabe b dieser Verordnung benannten Finanzunternehmens oder das gemäß Artikel 26 Absatz 4 der Verordnung (EU) 2022/2554 benannte Finanzunternehmen bewertet die Risiken in Verbindung mit der Beteiligung mehrerer Finanzunternehmen an dem TLPT. Die Kontrollteams der beteiligten Finanzunternehmen arbeiten mit dem Kontrollteam des

benannten Finanzunternehmens zusammen, um potenzielle gemeinsame Risiken zu ermitteln.“

Artikel 7 Absatz 2:

Anstatt: „(1) Das Kontrollteam führt Aufzeichnungen über die von den Testern und den Anbietern von Bedrohungsanalysen zum Nachweis der Einhaltung von Absatz 2 Buchstaben a bis f bereitgestellten Dokumente.

In Ausnahmefällen können Finanzunternehmen externe Tester und Anbieter von Bedrohungsanalysen beauftragen, die eine oder mehrere der in Absatz 2 Buchstaben a bis f genannten Anforderungen nicht erfüllen, sofern diese Finanzunternehmen geeignete Maßnahmen ergreifen, um die Risiken in Verbindung mit der Nichteinhaltung dieser Buchstaben zu mindern, und über diese Maßnahmen Aufzeichnungen führen.“

muss es heißen: „(2) Das Kontrollteam führt Aufzeichnungen über die von den Testern und den Anbietern von Bedrohungsanalysen zum Nachweis der Einhaltung von Absatz 1 Buchstaben a bis f bereitgestellten Dokumente.

In Ausnahmefällen können Finanzunternehmen externe Tester und Anbieter von Bedrohungsanalysen beauftragen, die eine oder mehrere der in Absatz 1 Buchstaben a bis f genannten Anforderungen nicht erfüllen, sofern diese Finanzunternehmen geeignete Maßnahmen ergreifen, um die Risiken in Verbindung mit der Nichteinhaltung dieser Buchstaben zu mindern, und über diese Maßnahmen Aufzeichnungen führen.“

Artikel 8 Absatz 1:

Anstatt: „(1) Sofern die federführende TLPT-Behörde nichts anderes beschließt, führt jedes Finanzunternehmen für den Fall, dass mehrere gemäß Artikel 16 Absätze 3 oder 4 ermittelte Finanzunternehmen an einem gebündelten oder gemeinsamen TLPT beteiligt sind, jeden der in den Artikeln 9 bis 15 genannten Schritte aus.“

muss es heißen: „(1) Sofern die federführende TLPT-Behörde nichts anderes beschließt, führt jedes Finanzunternehmen für den Fall, dass mehrere gemäß Artikel 16 Absätze 2 oder 4 ermittelte Finanzunternehmen an einem gebündelten oder gemeinsamen TLPT beteiligt sind, jeden der in den Artikeln 9 bis 15 genannten Schritte aus.“

Artikel 9 Absatz 1:

Anstatt: „(1) Ein nach Artikel 26 Absatz 8 Unterabsatz 2 der Verordnung (EU) 2022/2554 bestimmtes Finanzunternehmen leitet einen TLPT ein, nachdem es von der TLPT-Behörde eine Aufforderung zur Durchführung eines TLPT erhalten hat.“

muss es heißen: „(1) Ein nach Artikel 26 Absatz 8 Unterabsatz 3 der Verordnung (EU) 2022/2554 bestimmtes Finanzunternehmen leitet einen TLPT ein, nachdem es von der TLPT-Behörde eine Aufforderung zur Durchführung eines TLPT erhalten hat.“

Artikel 9 Absatz 6:

Anstatt: „(6) Das Finanzunternehmen legt den Testleitern innerhalb von sechs Monaten nach Eingang der Unterrichtung der TLPT-Behörde gemäß Absatz 2 ein Dokument zur Beschreibung des Testumfangs mit allen in Anhang II aufgeführten Informationen vor. Das Leitungsorgan des Finanzunternehmens genehmigt das Scoping-Dokument.“

muss es heißen: „(6) Das Finanzunternehmen legt den Testleitern innerhalb von sechs Monaten nach Eingang der Unterrichtung der TLPT-Behörde gemäß Absatz 1 ein Dokument zur Beschreibung des Testumfangs mit allen in Anhang II aufgeführten Informationen vor. Das Leitungsorgan des Finanzunternehmens genehmigt das Scoping-Dokument.“

Artikel 15 Absatz 3 Buchstabe a:

Anstatt: „a) Dokumente über die Einleitung des Tests gemäß Artikel 9“

muss es heißen: „a) Informationen über die Einleitung des Tests gemäß Artikel 9“

Artikel 16 Absatz 5 Buchstabe a:

Anstatt: „a) vereinbaren die für die Finanzunternehmen zuständigen TLPT-Behörden, welches Finanzunternehmen unter Berücksichtigung der IKT-Dienstleistungen, die der IKT-Drittdienstleister für die Finanzunternehmen erbringt, und der Wirksamkeit des Tests benannt wird, um die Durchführung des gebündelten TLPT zu leiten“

muss es heißen: „a) vereinbaren die für die Finanzunternehmen zuständigen TLPT-Behörden, welches Finanzunternehmen unter Berücksichtigung der IKT-Dienstleistungen, die der IKT-Drittdienstleister für die Finanzunternehmen erbringt, und der Wirksamkeit des Tests benannt wird, um den gebündelten TLPT durchzuführen“