



2025/1190

18.6.2025

**DELEGIERTE VERORDNUNG (EU) 2025/1190 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**

**(Text von Bedeutung für den EWR)**

DIE EUROPÄISCHE KOMMISSION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union,

gestützt auf die Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014, (EU) Nr. 909/2014 und (EU) 2016/1011<sup>(1)</sup>, insbesondere auf Artikel 26 Absatz 11 Unterabsatz 4,

in Erwägung nachstehender Gründe:

- (1) Diese Verordnung wurde im Einklang mit dem TIBER-EU-Rahmen ausgearbeitet und spiegelt die Methodik, das Verfahren und die Struktur bedrohungsorientierter Penetrationstests (im Folgenden „TLPT“) gemäß TIBER-EU wider. Finanzunternehmen, die zur Durchführung von TLPT verpflichtet sind, können sich auf den TIBER-EU-Rahmen oder eine seiner nationalen Umsetzungen beziehen und diesen Rahmen oder die nationale Umsetzung anwenden, sofern dieser Rahmen oder die Umsetzung mit den Anforderungen der Artikel 26 und 27 der Verordnung (EU) 2022/2554 und der vorliegenden Verordnung im Einklang steht. Die Benennung einer einzigen staatlichen Behörde für den Finanzsektor, die auf nationaler Ebene für mit TLPT verbundene Angelegenheiten zuständig ist, gemäß Artikel 26 Absatz 9 der Verordnung (EU) 2022/2554 sollte die auf Unionsebene den zuständigen Behörden übertragene Befugnis für die Beaufsichtigung bestimmter Finanzunternehmen gemäß Artikel 46 der genannten Verordnung unberührt lassen, wie beispielsweise die Zuständigkeit der Europäischen Zentralbank für bedeutende Kreditinstitute für mit TLPT verbundene Angelegenheiten. Werden nur einige mit TLPT verbundene Aufgaben gemäß Artikel 26 Absatz 10 der Verordnung (EU) 2022/2554 einer anderen nationalen Behörde für den Finanzsektor übertragen, so sollte die für das in Artikel 46 der genannten Verordnung genannte Finanzunternehmen zuständige Behörde für die nicht übertragenen mit TLPT verbundenen Aufgaben zuständig bleiben.
- (2) Angesichts der Komplexität des TLPT und der damit verbundenen Risiken sollte seine Durchführung auf diejenigen Finanzunternehmen beschränkt werden, bei denen er gerechtfertigt ist. Daher sollten die für mit TLPT verbundenen Angelegenheiten zuständigen Behörden (im Folgenden „TLPT-Behörden“) (auf Unions- oder auf nationaler Ebene) Finanzunternehmen vom Anwendungsbereich des TLPT ausnehmen, die in zentralen Finanzdienstleistungsteilsektoren tätig sind und bei denen ein TLPT nicht gerechtfertigt ist. Demnach könnten Kreditinstitute, Zahlungsinstitute, E-Geld-Institute, Zentralverwahrer, zentrale Gegenparteien, Handelsplätze, Versicherungs- und Rückversicherungsunternehmen unter Berücksichtigung einer Gesamtbewertung ihres IKT-Risikoprofils und ihres Reifegrads, ihrer Auswirkungen auf den Finanzsektor und entsprechender Bedenken hinsichtlich der Finanzstabilität von der Pflicht zur Durchführung von TLPT befreit werden, auch wenn sie die quantitativen Kriterien erfüllen.
- (3) Die TLPT-Behörden sollten unter Berücksichtigung einer Gesamtbewertung des IKT-Risikoprofils und des Reifegrads, der Auswirkungen auf den Finanzsektor und entsprechender Bedenken hinsichtlich der Finanzstabilität prüfen, ob andere Arten von Finanzunternehmen als Kreditinstitute, Zahlungsinstitute, E-Geld-Institute, zentrale Gegenparteien, Zentralverwahrer, Handelsplätze, Versicherungs- und Rückversicherungsunternehmen der Pflicht zur Durchführung von TLPT unterworfen werden sollten. Die Bewertung, ob diese Finanzunternehmen die genannten qualitativen Kriterien erfüllen, sollte darauf abzielen, anhand sektorübergreifender und objektiver Indikatoren diejenigen Finanzunternehmen zu ermitteln, die TLPT durchführen sollten. Gleichzeitig sollte die Bewertung, ob ein Finanzunternehmen diese qualitativen Kriterien erfüllt, darauf abzielen, TLPT auf diejenigen Unternehmen zu

<sup>(1)</sup> ABl. L 333 vom 27.12.2022, S. 1, ELI: <http://data.europa.eu/eli/reg/2022/2554/oj>.

beschränken, bei denen der Test gerechtfertigt ist. Ob ein Finanzunternehmen diese qualitativen Kriterien erfüllt, sollte auch vor dem Hintergrund neuer Marktentwicklungen und der künftigen zunehmenden Bedeutung neuer Marktteilnehmer für den Finanzsektor, einschließlich der gemäß Artikel 59 der Verordnung (EU) 2023/1114 des Europäischen Parlaments und des Rates <sup>(2)</sup> zugelassenen Anbieter von Krypto-Dienstleistungen, bewertet werden.

- (4) Finanzunternehmen können denselben gruppeninternen IKT-Dienstleister haben oder derselben Gruppe angehören und auf gemeinsame IKT-Systeme zurückgreifen. In diesem Fall ist es wichtig, dass die TLPT-Behörden bei der Beurteilung, ob ein Finanzunternehmen der Pflicht zur Durchführung von TLPT unterworfen werden sollte und ob der TLPT auf Unternehmensebene oder auf Gruppenebene (in Form eines gemeinsamen TLPT) durchgeführt werden sollte, die Struktur und den systemischen Charakter oder die Bedeutung des betreffenden Finanzunternehmens für den Finanzsektor auf nationaler oder Unionsebene berücksichtigen.
- (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).
- (6) Um sicherzustellen, dass in den TLPT die im Rahmen der Umsetzung von TIBER-EU gewonnenen Erfahrungen einfließen, und um die mit der Durchführung von TLPT verbundenen Risiken zu verringern, sollte sichergestellt werden, dass die Zuständigkeiten der TLPT-Cyberteams, die auf der Ebene der TLPT-Behörden eingerichtet werden, so weit wie möglich denen der TIBER-EU-Cyberteams entsprechen. Daher sollten für die TLPT-Cyberteams Testmanager bestimmt werden, die für die Beaufsichtigung der einzelnen TLPT sowie für die Planung und Koordinierung der einzelnen Tests verantwortlich sind. TLPT-Cyberteams sollten eine zentrale Anlaufstelle für die testbezogene Kommunikation mit internen und externen Interessenträgern, für die Sammlung und Verarbeitung von Rückmeldungen und Erkenntnissen aus bereits durchgeführten Tests und für die Unterstützung von Finanzunternehmen, bei denen ein TLPT durchgeführt wird, sein.
- (7) Um der Methodik des TIBER-EU-Rahmens Rechnung zu tragen, sollten Testmanager über die erforderlichen Fähigkeiten und Kompetenzen für die Begutachtung der Vorschläge der Tester und die entsprechende Beratung verfügen. Die Erfahrung im Rahmen des TIBER-EU-Rahmens hat gezeigt, dass es sinnvoll ist, jedem Test ein Team aus mindestens zwei Testmanagern zuzuweisen. Da mithilfe des TLPT die Lernerfahrung verbessert werden soll, und um die Vertraulichkeit der Tests zu wahren, wird den TLPT-Behörden dringend empfohlen, dafür zu sorgen, dass Testmanager während der Dauer eines TLPT keine Aufsichtstätigkeiten über das Finanzunternehmen, das sich einem TLPT unterzieht, ausüben (vorausgesetzt, bei den Behörden sind die nötigen Ressourcen oder Kompetenzen vorhanden).
- (8) Um dem TIBER-EU-Rahmen zu entsprechen, muss die TLPT-Behörde den Test in jeder einzelnen Phase genau verfolgen. Angesichts der Art des Tests und der damit verbundenen Risiken ist es von entscheidender Bedeutung, dass die TLPT-Behörde in jede einzelne Testphase einbezogen wird. Insbesondere sollte die TLPT-Behörde konsultiert werden und die Bewertungen oder Entscheidungen der Finanzunternehmen validieren, die zum einen die Wirksamkeit des Tests beeinflussen und sich zum anderen auf die mit dem Test verbundenen Risiken auswirken können. Zu den grundlegenden Schritten, bei denen eine spezifische Einbeziehung der TLPT-Behörde erforderlich ist, gehören die Validierung bestimmter grundlegender Bestandteile der Testdokumentation, die Auswahl von Anbietern von Bedrohungsanalysen und Testern sowie die Festlegung von Risikomanagementmaßnahmen. Die Einbeziehung der TLPT-Behörden, insbesondere bei Validierungen, sollte den Arbeitsaufwand dieser Behörden nicht übermäßig erhöhen und daher auf die Dokumente und Entscheidungen beschränkt bleiben, die sich unmittelbar auf die Durchführung des TLPT auswirken. Durch die aktive Einbeziehung in jede Testphase können die TLPT-Behörden effektiv bewerten, ob die Finanzunternehmen die einschlägigen Anforderungen erfüllen, und entsprechend die Bescheinigung gemäß Artikel 26 Absatz 7 der Verordnung (EU) 2022/2554 ausstellen.

<sup>(2)</sup> Verordnung (EU) 2023/1114 des Europäischen Parlaments und des Rates vom 31. Mai 2023 über Märkte für Kryptowerte und zur Änderung der Verordnungen (EU) Nr. 1093/2010 und (EU) Nr. 1095/2010 sowie der Richtlinien 2013/36/EU und (EU) 2019/1937 (ABl. L 150 vom 9.6.2023, S. 40, ELI: <http://data.europa.eu/eli/reg/2023/1114/oj>).

- (9) Die Geheimhaltung des TLPT ist äußerst wichtig, um sicherzustellen, dass die Testbedingungen realistisch sind. Aus diesem Grund sollten die Tests verdeckt erfolgen und es sollten Vorkehrungen getroffen werden, um die Vertraulichkeit des TLPT zu wahren. Beispielsweise sollten Codenamen so gewählt werden, dass eine Identifizierung des TLPT durch Dritte nicht möglich ist. Sollten Mitarbeiter, die für die Sicherheit des Finanzteams zuständig sind, von einem geplanten oder laufenden TLPT erfahren, sind sie wahrscheinlich aufmerksamer und wachsamer als unter normalen Arbeitsbedingungen, was zu einem anderen Testergebnis führen würde. Mitarbeiter des Finanzunternehmens, die nicht dem Kontrollteam angehören, sollten daher nur dann über geplante oder laufende TLPT informiert werden, wenn triftige Gründe vorliegen, und vorbehaltlich der vorherigen Zustimmung der Testmanager, um unter anderem die Geheimhaltung des Tests zu gewährleisten, falls ein Mitglied des Blue Teams den Test aufdeckt.
- (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.
- (11) Mit einem TLPT sind Risikokomponenten verbunden, da kritische Funktionen in einer Live-Produktionsumgebung getestet werden. Dies kann Denial-of-Service-Vorfälle, unerwartete Systemabstürze, Schäden an kritischen Live-Produktionssystemen oder den Verlust, die Veränderung oder die Offenlegung von Daten zur Folge haben. Diese Risiken machen deutlich, dass robuste Risikomanagementmaßnahmen erforderlich sind. Um sicherzustellen, dass der TLPT während der gesamten Testdauer kontrolliert durchgeführt wird, ist es sehr wichtig, dass sich die Finanzunternehmen jederzeit der besonderen Risiken bewusst sind, die mit einem TLPT verbunden sind, und dass diese Risiken gemindert werden. In diesem Zusammenhang kann unbeschadet der internen Prozesse des Finanzunternehmens und der Verantwortlichkeiten und Befugnisse, die dem Leiter des Kontrollteams bereits übertragen wurden, die Bereitstellung von Informationen über die TLPT-bezogenen Risikomanagementmaßnahmen oder — in besonderen Fällen — die Genehmigung dieser Risikomanagementmaßnahmen durch das Leitungsorgan des Finanzunternehmens geboten sein. Um effektive und qualifizierte professionelle Dienstleistungen erbringen zu können und diese Risiken zu mindern, ist es zudem von entscheidender Bedeutung, dass die Tester und die Anbieter von Bedrohungsanalysen (zusammen im Folgenden „TLPT-Anbieter“) über ein Höchstmaß an Fähigkeiten, Fachwissen und angemessene Erfahrung im Bereich Bedrohungsanalysen und TLPT in der Finanzdienstleistungsbranche verfügen.
- (12) Herkömmliche Penetrationstests ermöglichen eine detaillierte und hilfreiche Bewertung technischer und Konfigurationsschwachstellen, die häufig nur ein einzelnes System oder eine einzelne Umgebung betreffen und isoliert betrachtet werden. Im Gegensatz zu einem erkenntnisgestützten Red-Team-Test wird dabei nicht das gesamte Szenario eines gezielten Angriffs auf ein ganzes Unternehmen, einschließlich seiner Mitarbeiter, Prozesse und Technologien, bewertet. Bei der Auswahl der TLPT-Anbieter sollten Finanzunternehmen daher sicherstellen, dass diese Anbieter über die erforderlichen Fähigkeiten verfügen, um erkenntnisgestützte Red-Team-Tests durchzuführen, und nicht nur Penetrationstests. Es müssen daher umfassende Kriterien für interne und externe Tester sowie für Anbieter von Bedrohungsanalysen (immer extern) festgelegt werden. Gehören die TLPT-Anbieter demselben Unternehmen an, sollte sichergestellt werden, dass das für einen TLPT eingesetzte Personal angemessen von den übrigen Mitarbeitern getrennt ist.
- (13) In Ausnahmefällen kann es sein, dass ein Finanzunternehmen keine TLPT-Anbieter findet, die die umfassenden Kriterien erfüllen. Können Finanzunternehmen den Nachweis erbringen, dass solche Anbieter von Bedrohungsanalysen nicht verfügbar sind, sollten sie die Möglichkeit haben, Personen zu beauftragen, die nicht alle umfassenden Kriterien erfüllen, sofern sie die sich daraus ergebenden zusätzlichen Risiken angemessen mindern und die TLPT-Behörde sämtliche dieser Kriterien bewertet.
- (14) Sind mehrere Finanzunternehmen und mehrere TLPT-Behörden an einem TLPT beteiligt, sollten die Rollen aller am TLPT-Verfahren beteiligten Parteien festgelegt werden, damit der Test so effizient und sicher wie möglich durchgeführt wird. Bei gebündelten Tests müssen spezifische Anforderungen für die Festlegung der Rolle des benannten Finanzunternehmens gelten, d. h. dieses Finanzunternehmen sollte insbesondere dafür verantwortlich sein, der federführenden TLPT-Behörde alle erforderlichen Dokumente zur Verfügung zu stellen und das Testverfahren zu überwachen. Das benannte Finanzunternehmen sollte auch für die allgemeinen Aspekte der Risikomanagementbewertung verantwortlich sein. Ungeachtet der Rolle des benannten Finanzunternehmens sollten die Pflichten jedes Finanzunternehmens, das an dem gebündelten TLPT beteiligt ist, während des gebündelten Tests unberührt bleiben. Derselbe Grundsatz sollte auch für gemeinsame TLPT gelten.

- (15) Wie die Erfahrung mit der Umsetzung des TIBER-EU-Rahmens gezeigt hat, sind Präsenz- oder virtuelle Sitzungen mit allen betroffenen Interessenträger (Finanzunternehmen, Behörden, Tester und Anbieter von Bedrohungsanalysen) der effizienteste Weg, um eine angemessene Durchführung der Tests sicherzustellen. Daher sollten in verschiedenen Phasen des Prozesses Präsenz- und virtuelle Sitzungen abgehalten werden, das heißt während der Vorbereitungsphase zu Beginn des TLPT, um den Testumfang festzulegen, während der Testphase, um den Bedrohungsanalysebericht, den Red-Team-Testplan und die wöchentlichen Fortschrittsberichte zu erstellen, und während der Abschlussphase, um die Handlungen der Tester und des Blue Teams zu wiederholen, für das Purple-Teaming und um Rückmeldungen zu dem TLPT auszutauschen.
- (16) Um eine reibungslose Durchführung des TLPT zu gewährleisten, sollte die TLPT-Behörde dem Finanzunternehmen ihre Erwartungen in Bezug auf den Test klar darlegen. In diesem Zusammenhang sollten die Testmanager sicherstellen, dass ein angemessener Informationsfluss mit dem Kontrollteam innerhalb des Finanzunternehmens und mit den TLPT-Anbietern eingerichtet wird.
- (17) Das Finanzunternehmen sollte festlegen, welche kritischen oder wichtigen Funktionen in den Anwendungsbereich des TLPT fallen. Dabei sollte sich das Finanzunternehmen auf verschiedene Kriterien stützen, die sich auf die Bedeutung der jeweiligen Funktion für das Finanzunternehmen selbst und für den Finanzsektor auf Unions- und nationaler Ebene beziehen, und zwar nicht nur in wirtschaftlicher Hinsicht, sondern auch unter Berücksichtigung des symbolischen oder politischen Status der Funktion. Um einen reibungslosen Übergang zur Phase der Gewinnung von Bedrohungsinformationen zu erleichtern, sollte das Kontrollteam den nicht am Scoping-Verfahren beteiligten Testern und Anbietern von Bedrohungsanalysen detaillierte Informationen über den vereinbarten Testumfang zur Verfügung stellen.
- (18) Um den Testern die Informationen zur Verfügung zu stellen, die erforderlich sind, um einen realen und realistischen Angriff auf die Live-Systeme des Finanzunternehmens, die seinen kritischen oder wichtigen Funktionen zugrunde liegen, zu simulieren, sollte der Anbieter von Bedrohungsanalysen Erkenntnisse oder Informationen gewinnen, die mindestens zwei wichtige Interessenbereiche abdecken: die Angriffsziele, indem potenzielle Angriffsflächen im Finanzunternehmen ermittelt werden, und die Bedrohungen, indem relevante Angreifer und wahrscheinliche Bedrohungsszenarien ermittelt werden. Um sicherzustellen, dass der Anbieter von Bedrohungsanalysen die für das Finanzunternehmen relevanten Bedrohungen berücksichtigt, sollten die Tester, das Kontrollteam und die Testmanager Rückmeldungen zum Entwurf des Bedrohungsanalyseberichts geben. Sofern verfügbar, kann der Anbieter von Bedrohungsanalysen von der TLPT-Behörde für den Finanzsektor eines Mitgliedstaats bereitgestellte Informationen über die allgemeine Bedrohungslage als Ausgangsbasis für die nationale Bedrohungslage verwenden. Wird der TIBER-EU-Rahmen angewendet, dauert die Gewinnung von Bedrohungsinformationen in der Regel etwa vier Wochen.
- (19) Damit die Tester Einblicke gewinnen und das Scoping-Dokument und den spezifischen Bedrohungsanalysebericht weitergehend prüfen können, um den Red-Team-Testplan zu erstellen, ist es äußerst wichtig, dass die Tester vor der Red-Team-Testphase des TLPT vom Bedrohungsanalyse-Anbieter detaillierte Erläuterungen zu dem spezifischen Bedrohungsanalysebericht und zur Analyse möglicher Bedrohungsszenarien erhalten.
- (20) Damit die Tester einen realistischen und umfassenden Test durchführen können, bei dem alle Angriffsphasen durchgespielt und die vordefinierten Ziele (im Folgenden „Flags“) erreicht werden, sollte ausreichend Zeit für die aktive Red-Team-Testphase vorgesehen werden. Die Erfahrung mit dem TIBER-EU-Rahmen hat gezeigt, dass mindestens zwölf Wochen vorgesehen werden sollten; bei der Festlegung des Zeitrahmens sollten die Anzahl der beteiligten Parteien, der Umfang des TLPT, die Ressourcen des (der) beteiligten Finanzunternehmens(es), etwaige externe Anforderungen und die Verfügbarkeit der vom Finanzunternehmen bereitgestellten ergänzenden Informationen berücksichtigt werden.
- (21) Während der aktiven Red-Team-Testphase sollten die Tester eine Reihe von Taktiken, Techniken und Verfahren (im Folgenden „TTP“) anwenden, um die Live-Produktionssysteme des Finanzunternehmens angemessen zu testen. Die TTP sollten gegebenenfalls die Auskundschaftung (d. h. die Gewinnung möglichst vieler Informationen über das Angriffsziel — „Reconnaissance“), die Vorbereitung des Angriffs (d. h. die Analyse von Informationen über Infrastruktur, Einrichtungen und Mitarbeiter sowie die Vorbereitung der zielspezifischen Handlungen — „Weaponization“), die Platzierung des Schädlings (d. h. Beginn des Angriffs auf das Ziel — „Delivery“) und die Erlangung des Zugriffs (d. h. Kompromittierung der Server und Netzwerke des Finanzunternehmens und Verleitung seiner Mitarbeiter durch Social Engineering — „Exploitation“), Kontrolle und laterale Bewegung (d. h. Versuche, von den kompromittierten Systemen zu noch stärker gefährdeten oder wertvolleren Systemen überzugehen) und Erreichen des Angriffsziels (d. h. weiterer Zugriff auf kompromittierte Systeme und Zugang zu den Informationen und Daten des Angriffsziels, wie im Red-Team-Testplan vereinbart).

- (22) Bei der Durchführung eines TLPT sollten die Tester das für den Angriff zur Verfügung stehende Zeitbudget, die Ressourcen sowie ethische und rechtliche Grenzen berücksichtigen. Sollten die Tester nicht in der Lage sein, zur geplanten nächsten Angriffsphase überzugehen, sollte das Kontrollteam mit Zustimmung der TLPT-Behörde Unterstützung in Form von sogenannten „Hilfestellungen“ (Leg-up) leisten. Hilfestellungen können im Wesentlichen in den Bereichen Information und Zugang geleistet werden und darin bestehen, Zugang zu IKT-Systemen oder internen Netzwerken zu gewähren, damit der Test fortgesetzt werden und das Team sich auf die nachfolgenden Angriffsschritte konzentrieren kann.
- (23) Während des aktiven Red-Teamings in der Testphase sollte, falls dies erforderlich ist, um die Fortsetzung des TLPT zu ermöglichen, in Ausnahmefällen als letztes Mittel, und sofern alle alternativen Optionen ausgeschöpft wurden, auf eine gemeinsame Durchführung des Tests, an dem dann sowohl die Tester als auch das Blue Team teilnehmen, zurückgegriffen werden. Im Rahmen eines solchen Purple-Teaming, das auf Ausnahmefälle begrenzt ist, können folgende Methoden angewendet werden: „Catch-and-Release“, d. h. die Tester versuchen, die Szenarien fortzusetzen, werden entdeckt, und nehmen den Test anschließend wieder auf, „War Gaming“, das komplexere Szenarien ermöglicht, um strategische Entscheidungen zu testen, oder „Collaborative Proof-of-Concept“, der es Testern und Mitgliedern des Blue Teams ermöglicht, spezifische Sicherheitsmaßnahmen, -tools oder -techniken in einer kontrollierten und kooperativen Umgebung gemeinsam zu validieren.
- (24) Der TLPT sollte als Lernerfahrung genutzt werden, um die digitale operationale Resilienz von Finanzunternehmen zu verbessern. In diesem Zusammenhang sollten das Blue Team und die Tester den Angriff wiederholen und die durchgeführten Schritte analysieren, um in Zusammenarbeit mit den Testern Erkenntnisse aus den Tests zu gewinnen. Hierzu und um eine angemessene Vorbereitung zu ermöglichen, sollten der Red-Team-Testbericht und der Blue-Team-Testbericht allen an der Wiederholung beteiligten Parteien vor deren Durchführung zur Verfügung gestellt werden. Darüber hinaus sollte in der Abschlussphase ein Purple-Teaming stattfinden, um die Lernerfahrung zu maximieren. Die Methoden, die in der Abschlussphase für das Purple-Teaming verwendet werden können, sollten Diskussionen über alternative Angriffsszenarien, die Analyse alternativer Szenarien für Live-Systeme oder die erneute Analyse geplanter Szenarien für Live-Systeme umfassen, die die Tester während der Testphase nicht abschließen oder ausführen konnten.
- (25) Um die Lernerfahrung aller am TLPT beteiligten Parteien im Hinblick auf künftige Tests weiter zu verbessern und die digitale operationale Resilienz von Finanzunternehmen zu fördern, sollten die betroffenen Parteien einander Rückmeldungen zum gesamten Prozess geben und insbesondere ermitteln, welche Aktivitäten gut vorangekommen sind oder hätten verbessert werden können und welche Aspekte des TLPT-Verfahrens gut funktioniert haben oder verbessert werden könnten.
- (26) Die in Artikel 46 der Verordnung (EU) 2022/2554 genannten zuständigen Behörden und — falls davon abweichend — die TLPT-Behörden sollten zusammenarbeiten, um fortgeschrittene Tests in Form von TLPT in die bestehenden Aufsichtsverfahren einzubeziehen. In diesem Zusammenhang und um das korrekte Verständnis der aus dem TLPT gewonnenen Erkenntnisse und die Art und Weise der Interpretation zu kommunizieren, sollte insbesondere für den zusammenfassenden Testbericht und die Pläne mit Abhilfemaßnahmen eine enge Zusammenarbeit zwischen den am TLPT beteiligten Testmanagern und den zuständigen Aufsichtsbehörden stattfinden.
- (27) Nach Artikel 26 Absatz 8 Unterabsatz 1 der Verordnung (EU) 2022/2554 müssen Finanzunternehmen bei jedem dritten Test externe Tester beauftragen. Wenn Finanzunternehmen sowohl interne als auch externe Tester in das Testteam einbeziehen, ist dieser Test für die Zwecke des genannten Artikels als TLPT mit internen Testern zu betrachten.
- (28) Diese Verordnung beruht auf dem Entwurf technischer Regulierungsstandards, der der Kommission von der Europäischen Bankenaufsichtsbehörde, der Europäischen Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung und der Europäischen Wertpapier- und Marktaufsichtsbehörde (im Folgenden „Europäische Aufsichtsbehörden“) im Einvernehmen mit der Europäischen Zentralbank vorgelegt wurde.

- (29) Die Europäischen Aufsichtsbehörden haben zu diesem Entwurf offene öffentliche Konsultationen durchgeführt, die damit verbundenen potenziellen Kosten- und Nutzeneffekte analysiert und die Stellungnahme der nach Artikel 37 der Verordnung (EU) Nr. 1093/2010 des Europäischen Parlaments und des Rates <sup>(3)</sup> eingesetzten Interessengruppe „Bankensektor“, der nach Artikel 37 der Verordnung (EU) Nr. 1094/2010 des Europäischen Parlaments und des Rates <sup>(4)</sup> eingesetzten Interessengruppen „Versicherung und Rückversicherung“ und „Betriebliche Altersversorgung“ sowie der nach Artikel 37 der Verordnung (EU) Nr. 1095/2010 des Europäischen Parlaments und des Rates <sup>(5)</sup> eingesetzten Interessengruppe „Wertpapiere und Wertpapiermärkte“ eingeholt.
- (30) Der Europäische Datenschutzbeauftragte wurde gemäß Artikel 42 Absatz 1 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates <sup>(6)</sup> konsultiert und gab am 20. August 2024 eine Stellungnahme ab —

HAT FOLGENDE VERORDNUNG ERLASSEN:

### Artikel 1

#### Begriffsbestimmungen

Für die Zwecke dieser Verordnung bezeichnet der Ausdruck:

1. „Kontrollteam“ das Team, das sich aus Mitarbeitern des getesteten Finanzunternehmens und, entsprechend dem Umfang des TLPT, gegebenenfalls aus Mitarbeitern seiner Drittdienstleister und jeder anderen Partei, die den Test leitet, zusammensetzt;
2. „Leiter des Kontrollteams“ den Mitarbeiter des Finanzunternehmens, der für die Durchführung aller TLPT-bezogenen Aktivitäten des Finanzunternehmens im Rahmen eines bestimmten Tests verantwortlich ist;
3. „Blue Team“ die Mitarbeiter des Finanzunternehmens und gegebenenfalls die Mitarbeiter der Drittdienstleister des Finanzunternehmens und alle anderen entsprechend dem Umfang des TLPT als relevant erachteten Parteien bei den Drittdienstleistern des Finanzunternehmens, die die Nutzung von Netzwerk- und Informationssystemen des Finanzunternehmens absichern, indem sie seine Fähigkeit zur Abwehr simulierter oder realer Angriffe aufrechterhalten, und die keine Kenntnis vom TLPT haben;
4. „Blue-Team-Aufgaben“ Aufgaben, die in der Regel vom Blue Team wahrgenommen werden, wie z. B. Security Operation Centre (SOC), IKT-Infrastrukturdienstleistungen, Helpdesk-Dienstleistungen und Vorfallmanagement-Dienstleistungen auf operativer Ebene;
5. „Red Team“ die internen oder externen Tester, die mit einem TLPT beauftragt oder betraut wurden;
6. „Purple-Teaming“ gemeinsam durchgeführte Tests, an denen sowohl die Tester als auch das Blue Team beteiligt sind;

<sup>(3)</sup> Verordnung (EU) Nr. 1093/2010 des Europäischen Parlaments und des Rates vom 24. November 2010 zur Errichtung einer Europäischen Aufsichtsbehörde (Europäische Bankenaufsichtsbehörde), zur Änderung des Beschlusses Nr. 716/2009/EG und zur Aufhebung des Beschlusses 2009/78/EG der Kommission (ABl. L 331 vom 15.12.2010, S. 12, ELI: <http://data.europa.eu/eli/reg/2010/1093/oj>).

<sup>(4)</sup> Verordnung (EU) Nr. 1094/2010 des Europäischen Parlaments und des Rates vom 24. November 2010 zur Errichtung einer Europäischen Aufsichtsbehörde (Europäische Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung), zur Änderung des Beschlusses Nr. 716/2009/EG und zur Aufhebung des Beschlusses 2009/79/EG der Kommission (ABl. L 331 vom 15.12.2010, S. 48, ELI: <http://data.europa.eu/eli/reg/2010/1094/oj>).

<sup>(5)</sup> Verordnung (EU) Nr. 1095/2010 des Europäischen Parlaments und des Rates vom 24. November 2010 zur Errichtung einer Europäischen Aufsichtsbehörde (Europäische Wertpapier- und Marktaufsichtsbehörde), zur Änderung des Beschlusses Nr. 716/2009/EG und zur Aufhebung des Beschlusses 2009/77/EG der Kommission (ABl. L 331 vom 15.12.2010, S. 84, ELI: <http://data.europa.eu/eli/reg/2010/1095/oj>).

<sup>(6)</sup> Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG (ABl. L 295 vom 21.11.2018, S. 39, ELI: <http://data.europa.eu/eli/reg/2018/1725/oj>).

7. „TLPT-Behörde“ eine der folgenden Behörden:
  - a) die gemäß Artikel 26 Absatz 9 der Verordnung (EU) 2022/2554 benannte einzige staatliche Behörde im Finanzsektor,
  - b) die für den Finanzsektor zuständige Behörde, der die Wahrnehmung einiger oder aller Aufgaben im Zusammenhang mit TLPT gemäß Artikel 26 Absatz 10 der Verordnung (EU) 2022/2554 übertragen wird,
  - c) eine der in Artikel 46 der Verordnung (EU) 2022/2554 genannten zuständigen Behörden;
8. „TLPT-Cyberteams“ oder „TCT“ die Mitarbeiter der TLPT-Behörden, die für mit TLPT verbundene Angelegenheiten zuständig sind;
9. „Testmanager“ die Mitarbeiter, die benannt wurden, um die Aktivitäten der TLPT-Behörde für einen bestimmten TLPT zu leiten und die Einhaltung dieser Verordnung zu überwachen;
10. „Anbieter von Bedrohungsanalysen“ die Sachverständigen, die vom Finanzunternehmen für den jeweiligen TLPT beauftragt wurden und nicht dem Finanzunternehmen oder etwaigen gruppeninternen IKT-Dienstleistern angehören und die gezielte Bedrohungsinformationen sammeln und analysieren, welche für die Finanzunternehmen, die in den Anwendungsbereich eines spezifischen TLPT fallen, relevant sind, und entsprechende relevante und realistische Bedrohungsszenarien entwickeln;
11. „TLPT-Anbieter“ Tester und Anbieter von Bedrohungsanalysen;
12. „Hilfestellung“ oder „Leg-up“ die Unterstützung oder Informationen, die das Kontrollteam den Testern zur Verfügung stellt, um es ihnen zu ermöglichen, einen Angriffspfad fortzusetzen, wenn sie allein nicht weiterkommen, und wenn es keine andere vernünftige Alternative gibt, z. B. wenn für einen TLPT nicht genug Zeit oder Ressourcen zur Verfügung stehen;
13. „Angriffspfad“ den Pfad, dem die Tester während des aktiven Red-Team-Tests folgen, um die für diesen TLPT vordefinierten Ziele zu erreichen;
14. „Flags“ oder „vordefinierte Ziele“ Kernziele der IKT-Systeme zur Unterstützung kritischer oder wichtiger Funktionen eines Finanzunternehmens, die die Tester mit dem Test zu erreichen versuchen;
15. „sensible Informationen“ Informationen, die leicht für Angriffe auf die IKT-Systeme des Finanzunternehmens genutzt werden können, geistiges Eigentum, vertrauliche Geschäftsdaten oder personenbezogene Daten, die dem Finanzunternehmen und seinem Ökosystem direkt oder indirekt schaden könnten, wenn sie in die Hände böswilliger Akteure fallen würden;
16. „Pool“ alle Finanzunternehmen, die an einem gebündelten TLPT gemäß Artikel 26 Absatz 4 der Verordnung (EU) 2022/2554 teilnehmen;
17. „Aufnahmemitgliedstaat“ den Aufnahmemitgliedstaat gemäß den sektorspezifischen Rechtsvorschriften der Union, die für das betreffende Finanzunternehmen gelten;
18. „gemeinsamer TLPT“ einen TLPT, bei dem es sich nicht um einen gebündelten TLPT im Sinne des Artikels 26 Absatz 4 der Verordnung (EU) 2022/2554 handelt und an dem mehrere Finanzunternehmen beteiligt sind, die denselben gruppeninternen IKT-Dienstleister in Anspruch nehmen oder derselben Gruppe angehören und IKT-Systeme gemeinsam nutzen.

## Artikel 2

### **Bestimmung der Finanzunternehmen, die zur Durchführung eines TLPT verpflichtet sind**

(1) Die TLPT-Behörden prüfen, ob ein Finanzunternehmen zur Durchführung eines TLPT verpflichtet ist, und berücksichtigen dabei die Auswirkungen dieses Finanzunternehmens, seinen systemischen Charakter und sein IKT-Risikoprofil auf der Grundlage aller folgenden Kriterien:

- a) Faktoren in Verbindung mit Auswirkungen und systemischem Charakter:
  - i) Größe des Finanzunternehmens, die sich danach richtet, ob das Finanzunternehmen Finanzdienstleistungen in einem oder mehreren Mitgliedstaaten erbringt, und die durch Vergleich der Tätigkeiten des Finanzunternehmens mit denen anderer Finanzunternehmen, die ähnliche Dienstleistungen erbringen, ermittelt wird,
  - ii) Ausmaß und Art der Verflechtung des Finanzunternehmens mit anderen Finanzunternehmen des Finanzsektors in einem oder mehreren Mitgliedstaaten,
  - iii) Kritikalität oder Bedeutung der Dienstleistungen, die das Finanzunternehmen für den Finanzsektor erbringt,

- iv) Substituierbarkeit der von dem betreffenden Finanzunternehmen erbrachten Dienstleistungen,
  - v) Komplexität des Geschäftsmodells des Finanzunternehmens und der damit verbundenen Dienstleistungen und Prozesse,
  - vi) Frage, ob das Finanzunternehmen Teil einer Gruppe systemischen Charakters auf Unionsebene oder auf nationaler Ebene im Finanzsektor ist und IKT-Systeme gemeinsam nutzt;
- b) Faktoren in Verbindung mit dem IKT-Risiko:
- i) Risikoprofil des Finanzunternehmens,
  - ii) Bedrohungslage des Finanzunternehmens,
  - iii) Grad der Abhängigkeit kritischer oder wichtiger Funktionen des Finanzunternehmens oder seiner unterstützenden Funktionen von IKT-Systemen und -Prozessen,
  - iv) Komplexität der IKT-Architektur des Finanzunternehmens,
  - v) Von IKT-Drittdienstleistern unterstützte IKT-Dienstleistungen und -Funktionen sowie Anzahl und Art der vertraglichen Vereinbarungen mit IKT-Drittdienstleistern oder gruppeninternen IKT-Dienstleistern,
  - vi) Ergebnisse etwaiger aufsichtlicher Überprüfungen, die für die Bewertung der IKT-Reife des Finanzunternehmens relevant sind,
  - vii) Reifegrad der IKT-Geschäftsfortführungspläne und IKT-Reaktions- und Wiederherstellungspläne,
  - viii) Reifegrad der operativen IKT-Sicherheitskontrollen und Risikominderungsmaßnahmen, einschließlich der Fähigkeit,
    1. die IKT-Infrastruktur des Finanzunternehmens dauerhaft zu überwachen,
    2. IKT-bezogene Ereignisse in Echtzeit zu erkennen,
    3. die unter Ziffer 2 genannten Ereignisse zu analysieren,
    4. auf die unter Ziffer 2 genannten Ereignisse schnell und wirksam zu reagieren,
  - ix) Frage, ob das Finanzunternehmen Teil einer Gruppe ist, die auf Unionsebene oder auf nationaler Ebene im Finanzsektor tätig ist und IKT-Systeme gemeinsam nutzt.

Für die Zwecke des Buchstabens a Ziffer i berücksichtigt die TLPT-Behörde nach Möglichkeit

- a) den Marktanteil des Finanzunternehmens auf Unions- und nationaler Ebene,
- b) das Spektrum der vom Finanzunternehmen angebotenen Tätigkeiten,
- c) den Marktanteil der vom Finanzunternehmen erbrachten Dienstleistungen oder der auf Unions- und nationaler Ebene durchgeführten Tätigkeiten.

Für die Zwecke des Buchstabens a Ziffer v berücksichtigt die TLPT-Behörde, soweit möglich,

- a) ob das Finanzunternehmen über mehr als ein Geschäftsmodell verfügt,
- b) die Verflechtung der verschiedenen Geschäftsprozesse und der damit verbundenen Dienstleistungen.

(2) Die TLPT-Behörden verlangen von allen folgenden Finanzunternehmen die Durchführung von TLPT, es sei denn, die Bewertung eines Finanzunternehmens gemäß Absatz 1 hat ergeben, dass seine Auswirkungen, Bedenken hinsichtlich der Finanzstabilität in Bezug auf das betreffende Finanzunternehmen oder sein IKT-Risikoprofil die Durchführung eines TLPT nicht rechtfertigen:

- a) Kreditinstitute, die eine der folgenden Bedingungen erfüllen:
  - i) Sie wurden gemäß Artikel 131 der Richtlinie 2013/36/EU des Europäischen Parlaments und des Rates<sup>(7)</sup> als global systemrelevante Institute (G-SRI) eingestuft.
  - ii) Sie wurden gemäß Artikel 131 der Richtlinie 2013/36/EU als andere systemrelevante Institute („A-SRI“) ermittelt.
  - iii) Sie sind Teil eines G-SRI oder A-SRI.

(7) Richtlinie 2013/36/EU des Europäischen Parlaments und des Rates vom 26. Juni 2013 über den Zugang zur Tätigkeit von Kreditinstituten und die Beaufsichtigung von Kreditinstituten und Wertpapierfirmen, zur Änderung der Richtlinie 2002/87/EG und zur Aufhebung der Richtlinien 2006/48/EG und 2006/49/EG (ABl. L 176 vom 27.6.2013, S. 338, ELI: <http://data.europa.eu/eli/dir/2013/36/oj>).

- b) Zahlungsinstitute, die in jedem der beiden Kalenderjahre, die der Bewertung durch die TLPT-Behörde vorausgehen, einen Gesamtbetrag der Zahlungsvorgänge im Sinne von Artikel 4 Ziffer 5 der Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates <sup>(8)</sup> von 150 Mrd. EUR überschritten haben,
- c) E-Geld-Institute, die in jedem der beiden Kalenderjahre, die der Bewertung durch die TLPT-Behörde vorausgehen, entweder einen Gesamtbetrag der Zahlungsvorgänge im Sinne von Artikel 4 Ziffer 5 der Richtlinie (EU) 2015/2366 von 150 Mrd. EUR oder einen Gesamtbetrag des E-Geld-Umlaufs von 40 Mrd. EUR überschritten haben,
- d) Zentralverwahrer,
- e) zentrale Gegenparteien,
- f) Handelsplätze mit einem elektronischen Handelssystem, die eines der folgenden Kriterien erfüllen:
- i) Der Handelsplatz hat in jedem der beiden Kalenderjahre, die der Bewertung durch die TLPT-Behörde vorausgehen, in Bezug auf den Umsatz auf nationaler Ebene den höchsten Marktanteil in einem der folgenden Bereiche:
1. übertragbare Wertpapiere im Sinne des Artikels 4 Absatz 1 Nummer 44 Buchstabe a der Richtlinie 2014/65/EU des Europäischen Parlaments und des Rates <sup>(9)</sup>,
  2. übertragbare Wertpapiere im Sinne des Artikels 4 Absatz 1 Nummer 44 Buchstabe b der Richtlinie 2014/65/EU,
  3. Derivate im Sinne des Artikels 2 Absatz 1 Nummer 29 der Verordnung (EU) Nr. 600/2014 des Europäischen Parlaments und des Rates <sup>(10)</sup>,
  4. strukturierte Finanzprodukte im Sinne des Artikels 2 Absatz 1 Nummer 28 der Verordnung (EU) Nr. 600/2014,
  5. Emissionszertifikate im Sinne des Anhangs I Abschnitt C Nummer 11 der Richtlinie 2014/65/EU,
- ii) Der Handelsplatz hat in jedem der beiden Kalenderjahre, die der Bewertung durch die TLPT-Behörde vorausgehen, in Bezug auf den Umsatz auf Unionsebene einen Marktanteil von über 5 % in einem der folgenden Bereiche:
1. Aktien und andere, Aktien oder Anteilen an Gesellschaften, Personengesellschaften oder anderen Rechtspersonlichkeiten gleichzustellende Wertpapiere sowie Aktienzertifikate,
  2. Schuldverschreibungen oder andere verbrieftete Schuldtitel, einschließlich Zertifikaten (Hinterlegungsscheinen) für solche Wertpapiere,
  3. Derivate, die in Artikel 2 Absatz 1 Nummer 29 der Verordnung (EU) Nr. 600/2014 definiert sind,
  4. strukturierte Finanzprodukte im Sinne des Artikels 2 Absatz 1 Nummer 28 der Verordnung (EU) Nr. 600/2014,
  5. Emissionszertifikate im Sinne des Anhangs I Abschnitt C Nummer 11 der Richtlinie 2014/65/EU.

<sup>(8)</sup> Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates vom 25. November 2015 über Zahlungsdienste im Binnenmarkt, zur Änderung der Richtlinien 2002/65/EG, 2009/110/EG und 2013/36/EU und der Verordnung (EU) Nr. 1093/2010 sowie zur Aufhebung der Richtlinie 2007/64/EG (ABl. L 337 vom 23.12.2015, S. 35, ELI: <http://data.europa.eu/eli/dir/2015/2366/oj>).

<sup>(9)</sup> Richtlinie 2014/65/EU des Europäischen Parlaments und des Rates vom 15. Mai 2014 über Märkte für Finanzinstrumente sowie zur Änderung der Richtlinien 2002/92/EG und 2011/61/EU (ABl. L 173 vom 12.6.2014, S. 349, ELI: <http://data.europa.eu/eli/dir/2014/65/oj>).

<sup>(10)</sup> Verordnung (EU) Nr. 600/2014 des Europäischen Parlaments und des Rates vom 15. Mai 2014 über Märkte für Finanzinstrumente und zur Änderung der Verordnung (EU) Nr. 648/2012 (ABl. L 173 vom 12.6.2014, S. 84, ELI: <http://data.europa.eu/eli/reg/2014/600/oj>).

- g) Versicherungs- und Rückversicherungsunternehmen, die alle folgenden Kriterien erfüllen:
- i) Die verbuchten Bruttoprämieneinnahmen betragen mehr als 1 500 000 000 EUR.
  - ii) Die versicherungstechnischen Rückstellungen betragen mehr als 10 000 000 000 EUR.
  - iii) Versicherungsunternehmen, die nur in der Lebensversicherung oder die sowohl in der Lebensversicherung als auch in der Nichtlebensversicherung tätig sind und deren Vermögenswerte insgesamt 3,5 % der Summe der gemäß Artikel 75 der Richtlinie 2009/138/EG des Europäischen Parlaments und des Rates bewerteten gesamten Vermögenswerte <sup>(1)</sup> der in dem Mitgliedstaat niedergelassenen Versicherungs- und Rückversicherungsunternehmen übersteigen.

Für die Zwecke des Buchstabens f Ziffer ii wird für den Fall, dass der Handelsplatz Teil eines gruppenübergreifenden IKT-Systems oder desselben gruppeninternen IKT-Dienstleisters ist, der Umsatz mit den Wertpapieren und Derivatkontrakten an allen Handelsplätzen berücksichtigt, die derselben Gruppe angehören und in der Union niedergelassen sind.

Für die Zwecke des Buchstabens g ermitteln die TLPT-Behörden eine Untergruppe aller Versicherungs- und Rückversicherungsunternehmen und wenden die unter Buchstabe g Ziffern i, ii und iii festgelegten Kriterien an. Zu dieser Untergruppe gehörende Versicherungs- und Rückversicherungsunternehmen sind zur Durchführung von TLPT verpflichtet, wenn sie eines der folgenden Kriterien erfüllen:

- a) verbuchte Bruttoprämieneinnahmen von mehr als 3 000 000 000 EUR,
- b) versicherungstechnische Rückstellungen von mehr als 30 000 000 000 EUR,
- c) Summe der Vermögenswerte übersteigt 10 % der Summe der gemäß Artikel 75 der Richtlinie 2009/138/EG bewerteten gesamten Vermögenswerte der in dem Mitgliedstaat niedergelassenen Versicherungs- und Rückversicherungsunternehmen.

(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.

Unterscheidet sich die für das Mutterunternehmen einer in Unterabsatz 1 genannten Gruppe von Finanzunternehmen zuständige TLPT-Behörde von den für die Finanzunternehmen der Gruppe zuständigen TLPT-Behörden, so wird diese Behörde von den TLPT-Behörden, die für die zu dieser Gruppe gehörenden Finanzunternehmen zuständig sind, zu der Frage konsultiert, ob TLPT auf Einzelbasis durchgeführt werden sollten.

### Artikel 3

#### TCT- und TLPT-Testmanager

- (1) Eine TLPT-Behörde überträgt die Zuständigkeit für die Koordinierung der mit TLPT verbundenen Aktivitäten einem Test-Cyberteam (im Folgenden „TCT“). Ein TCT setzt sich aus Testmanagern zusammen, die mit der Beaufsichtigung eines einzelnen TLPT betraut sind.
- (2) Für jeden Test benennt die TLPT-Behörde einen Testmanager und mindestens einen Stellvertreter.
- (3) Die Testmanager überwachen, ob die in dieser Verordnung festgelegten Anforderungen eingehalten werden, und stellen deren Einhaltung sicher.

<sup>(1)</sup> Richtlinie 2009/138/EG des Europäischen Parlaments und des Rates vom 25. November 2009 betreffend die Aufnahme und Ausübung der Versicherungs- und der Rückversicherungstätigkeit (Solvabilität II) (ABl. L 335 vom 17.12.2009, S. 1, ELI: <http://data.europa.eu/eli/dir/2009/138/oj>).

- (4) Der Testmanager teilt dem Finanzunternehmen die Kontaktdaten des TCT im Wege der in Artikel 9 Absatz 1 genannten Aufforderung mit.
- (5) Die TLPT-Behörde nimmt an allen Phasen des TLPT teil.

#### Artikel 4

### Von den Finanzunternehmen zu treffende organisatorische Vorkehrungen

- (1) Die Finanzunternehmen benennen ein Kontrollteam, das für die laufende Umsetzung des TLPT sowie die Entscheidungen und Maßnahmen des Kontrollteams zuständig ist.
- (2) Finanzunternehmen legen organisatorische und verfahrenstechnische Maßnahmen fest, um sicherzustellen, dass
  - a) der Zugang zu Informationen über geplante oder laufende TLPT dem Kontrollteam, dem Leitungsorgan, den Testern, dem Anbieter von Bedrohungsanalysen und der TLPT-Behörde nur in dem Maße gewährt wird, in dem die Kenntnis der Informationen notwendig ist,
  - b) das Kontrollteam die Testmanager konsultiert, bevor es ein Mitglied des Blue Teams in einen TLPT einbindet,
  - c) das Kontrollteam informiert wird, wenn ein Mitarbeiter des Finanzunternehmens oder seiner Drittdienstleister den TLPT aufdeckt, im Falle einer Eskalation der sich daraus ergebenden Reaktion auf Vorfälle das Kontrollteam erforderlichenfalls eine solche Eskalation eindämmt,
  - d) Vereinbarungen über die Geheimhaltung des TLPT bestehen, die für die Mitarbeiter des Finanzunternehmens, die Mitarbeiter der betreffenden IKT-Drittdienstleister, Tester und den Anbieter von Bedrohungsanalysen gelten,
  - e) das Kontrollteam den Testmanagern auf Anfrage alle Informationen über den TLPT zur Verfügung stellt,
  - f) sich die am TLPT beteiligten Parteien nach Möglichkeit nur mit Codenamen darauf beziehen.

#### Artikel 5

### Risikomanagement bei TLPT

- (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
  - a) den Finanzsektor,
  - b) die Finanzstabilität auf Unions- oder nationaler Ebene.

Das Kontrollteam überprüft diese Auswirkungen während des gesamten Tests.

- (2) Für die Zwecke der Risikobewertung und des Risikomanagements berücksichtigt das Kontrollteam mindestens die folgenden Arten von Risiken in Verbindung mit
  - a) der Gewährung des Zugangs zu sensiblen Informationen über das Finanzunternehmen für die Anbieter von Bedrohungsanalysen und gegebenenfalls externe Tester,
  - b) der unzureichenden Einhaltung der Verordnung (EU) 2022/2554 und der vorliegenden Verordnung bei der Durchführung des TLPT, wenn diese unzureichende Einhaltung dazu führt, dass die in Artikel 26 Absatz 7 der Verordnung (EU) 2022/2554 genannte Bescheinigung nicht ausgestellt wird, auch wenn diese unzureichende Einhaltung auf Verletzungen der Vertraulichkeit des TLPT oder mangelndes ethisches Verhalten zurückzuführen ist,
  - c) einer Eskalation in eine Krise oder einen Vorfall,
  - d) der aktiven Red-Team-Phase, einschließlich der Risiken in Verbindung mit der Unterbrechung kritischer Tätigkeiten und der Datenkorruption aufgrund der Aktivitäten der Tester, und ihrer potenziellen Auswirkungen auf Dritte,

- e) der Aktivität des Blue Teams, einschließlich der Risiken in Verbindung mit der Unterbrechung kritischer Tätigkeiten und der Datenkorruption aufgrund der Aktivitäten des Blue Teams, und ihrer potenziellen Auswirkungen auf Dritte,
- f) der unvollständigen Wiederherstellung der vom TLPT betroffenen Systeme.

#### Artikel 6

### Risikomanagement bei gebündelten oder gemeinsamen TLPT

- (1) Im Falle eines gemeinsamen TLPT oder eines gebündelten TLPT führt das Kontrollteam jedes Finanzunternehmens eine eigene Risikobewertung durch und legt seine eigenen Risikomanagementmaßnahmen fest.
- (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

### Auswahl der TLPT-Anbieter

- (1) Das Kontrollteam ergreift Maßnahmen zur Steuerung der mit dem TLPT verbundenen Risiken und stellt insbesondere sicher, dass bei jedem TLPT
  - a) der Anbieter von Bedrohungsanalysen und externe Tester dem Kontrollteam einen ausführlichen Lebenslauf und Kopien von Bescheinigungen vorlegen, die nach anerkannten Marktstandards eine geeignete Grundlage für die Durchführung ihrer Tätigkeiten sind,
  - b) der Anbieter von Bedrohungsanalysen und externe Tester ordnungsgemäß und vollständig durch einschlägige Berufshaftpflichtversicherungen abgesichert sind, einschließlich einer Versicherung gegen das Risiko von Fehlverhalten und Fahrlässigkeit,
  - c) der Anbieter von Bedrohungsanalysen mindestens drei Referenzen aus früheren Aufträgen im Zusammenhang mit Penetrationstests und Red-Team-Testing vorlegt,
  - d) die externen Tester mindestens fünf Referenzen aus früheren Aufträgen im Zusammenhang mit Penetrationstests und Red-Team-Testing vorlegen,
  - e) die dem TLPT zugewiesenen Mitarbeiter des Anbieters von Bedrohungsanalysen
    - i) aus mindestens einer Führungskraft mit mindestens fünf Jahren Erfahrung im Bereich der Bedrohungsanalyse und mindestens einem weiteren Mitglied mit mindestens zwei Jahren Erfahrung im Bereich der Bedrohungsanalyse besteht,
    - ii) ein breites und angemessenes Niveau an Fachkenntnissen und beruflichen Qualifikationen aufweist, darunter
      - 1. Kenntnis der Taktiken, Techniken und Verfahren zur Informationsgewinnung,
      - 2. geopolitisches, technisches und sektorbezogenes Wissen,
      - 3. angemessene Kommunikationsfähigkeiten, um das Ergebnis des Arbeitsauftrags klar darzulegen und darüber Bericht zu erstatten,
    - iii) in der Vergangenheit an insgesamt mindestens drei Arbeitsaufträgen im Bereich der Bedrohungsanalyse im Zusammenhang mit Penetrationstests und Red-Team-Tests beteiligt war,
    - iv) nicht gleichzeitig Blue-Team-Aufgaben oder andere Dienstleistungen ausführt, die einen Interessenkonflikt hinsichtlich des an dem TLPT, dem sie zugewiesen sind, beteiligten Finanzunternehmens, IKT-Drittdienstleisters oder gruppeninternen IKT-Dienstleisters darstellen könnten,
    - v) von Mitarbeitern desselben TLPT-Anbieters, der externe Tester für denselben TLPT bereitstellt, getrennt ist und diesen nicht Bericht erstattet,

- f) bei externen Testern das dem TLPT zugewiesene Red Team
  - i) aus mindestens einer Führungskraft mit mindestens fünf Jahren Erfahrung mit Penetrationstests und Red-Team-Tests sowie mindestens zwei weiteren Testern, die jeweils mindestens zwei Jahre Erfahrung mit Penetrationstests und Red-Team-Tests haben, besteht,
  - ii) ein breites und angemessenes Niveau an Fachkenntnissen und beruflichen Qualifikationen aufweist, darunter Kenntnisse über die Geschäftstätigkeit des Finanzunternehmens, Auskundenschaftung, Risikomanagement, Exploit-Entwicklung, physische Penetration, Social Engineering und Schwachstellenanalyse, und angemessene Kommunikationsfähigkeiten besitzt, um das Ergebnis des Arbeitsauftrags klar darzulegen und darüber Bericht zu erstatten,
  - iii) in der Vergangenheit an insgesamt mindestens fünf Arbeitsaufträgen im Zusammenhang mit Penetrationstests und Red-Team-Tests beteiligt war,
  - iv) weder bei einem Anbieter von Bedrohungsanalysen, der gleichzeitig Blue-Team-Aufgaben für ein an dem TLPT beteiligtes Finanzunternehmen, einen IKT-Drittdienstleister oder einen gruppeninternen IKT-Dienstleister wahrnimmt, beschäftigt ist noch Dienstleistungen für einen solchen Anbieter erbringt,
  - v) von Mitarbeitern desselben TLPT-Anbieters getrennt ist, der gleichzeitig Bedrohungsanalyse-Dienstleistungen für denselben TLPT erbringt,
- g) die Tester und der Anbieter von Bedrohungsanalysen am Ende der Tests Wiederherstellungsverfahren durchführen, einschließlich der sicheren Löschung von Informationen im Zusammenhang mit Passwörtern, Zugangsdaten und anderen geheimen Schlüsseln, die während des TLPT kompromittiert wurden, der sicheren Kommunikation mit den Finanzunternehmen über die kompromittierten Konten, der sicheren Erfassung, Speicherung, Verwaltung und Vernichtung anderer während der Tests erhobener Daten,
- h) die Tester zusätzlich zu den Wiederherstellungsverfahren am Ende der Tests gemäß Buchstabe g die folgenden Wiederherstellungsverfahren durchführen:
  - i) Deaktivierung von Command-and-Control-Diensten,
  - ii) Kill Switches für Umfang und Datum,
  - iii) Entfernung von Hintertüren und anderer Schadsoftware,
  - iv) Meldung möglicher Sicherheitsverletzungen,
  - v) Verfahren für die künftige Backup-Wiederherstellung, die während des Tests installierte Schadsoftware oder Tools betreffen können,
  - vi) Überwachung der Aktivitäten des Blue Teams und Unterrichtung des Kontrollteams, wenn der Test aufgedeckt wird,
- i) die Tester und der Anbieter von Bedrohungsanalysen keine der folgenden Aktivitäten durchführen oder sich daran beteiligen:
  - i) unbefugte Zerstörung von Ausrüstung des Finanzunternehmens und gegebenenfalls seiner IKT-Drittdienstleister,
  - ii) unkontrollierte Veränderung der Informationen und IKT-Ressourcen des Finanzunternehmens und gegebenenfalls seiner IKT-Drittdienstleister,
  - iii) vorsätzliche Gefährdung der Kontinuität kritischer oder wichtiger Funktionen des Finanzunternehmens,
  - iv) unbefugte Einbeziehung von Systemen, die nicht in den Anwendungsbereich fallen,
  - v) unbefugte Offenlegung der Testergebnisse.

(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

### **Besondere Anforderungen bei gebündelten oder gemeinsamen TLPT**

(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.

(2) Sofern in dieser Verordnung nichts anderes bestimmt ist, sind für den Fall, dass mehrere TLPT-Behörden an einem gemeinsamen TLPT oder einem gebündelten TLPT gemäß Artikel 16 Absatz 3 oder Artikel 16 Absatz 5 beteiligt sind, Bezugnahmen auf „TLPT-Behörde“ in den Artikeln 9 bis 15 als Bezugnahme auf die federführende TLPT-Behörde für einen solchen gebündelten oder gemeinsamen TLPT zu verstehen.

#### Artikel 9

### **Vorbereitungsphase**

(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.

(2) Das Finanzunternehmen übermittelt den Testmanagern innerhalb von drei Monaten nach Erhalt der in Absatz 1 genannten Aufforderung alle folgenden Informationen über die Einleitung des TLPT:

- a) Projektcharta mit einem übergeordneten Projektplan, der die in Anhang I aufgeführten Angaben enthält,
- b) Kontaktdaten des Leiters des Kontrollteams,
- c) Informationen über den beabsichtigten Einsatz interner oder externer Tester oder beidem, wie in Artikel 15 dargelegt,
- d) Angaben zu den Kommunikationskanälen, die während des TLPT genutzt werden sollen,
- e) Codename für den TLPT.

(3) Sind die in Absatz 2 Buchstaben a bis e genannten Informationen vollständig und stellen die Angemessenheit und wirksame Durchführung des TLPT sicher, so validiert die TLPT-Behörde die vom Finanzunternehmen vorgelegten Informationen, die die Einleitung des TLPT betreffen, und unterrichtet das Finanzunternehmen über die Validierung.

(4) Nach der Validierung der Informationen über die Einleitung des TLPT durch die TLPT-Behörde richtet das Finanzunternehmen ein Kontrollteam ein, das den Leiter des Kontrollteams bei seinen folgenden Aufgaben unterstützt:

- a) Festlegung von Kommunikationskanälen und -prozessen innerhalb des Kontrollteams, mit den Testern und den Anbietern von Bedrohungsanalysen in allen mit dem TLPT verbundenen Belangen,
- b) Unterrichtung des Leitungsorgans des Finanzunternehmens über den Fortgang des TLPT und die damit verbundenen Risiken,
- c) Entscheidungsfindung auf der Grundlage von Fachkompetenz während des gesamten TLPT,
- d) Durchführung des TLPT im Einklang mit dieser Verordnung,
- e) Auswahl des Anbieters von Bedrohungsanalysen für den TLPT,
- f) Auswahl der externen Tester, der internen Tester oder beidem,
- g) Ausarbeitung des Scoping-Dokuments zur Festlegung des Testumfangs.

(5) Ist die TLPT-Behörde der Auffassung, dass die anfängliche Zusammensetzung des Kontrollteams und etwaige spätere Änderungen der Zusammensetzung für die Erfüllung der in Absatz 4 genannten Aufgaben angemessen sind, so validiert die TLPT-Behörde das Kontrollteam und unterrichtet den Leiter des Kontrollteams über diese Validierung.

(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.

(7) Die Finanzunternehmen berücksichtigen bei der Einbeziehung kritischer oder wichtiger Funktionen in den Anwendungsbereich des TLPT die folgenden Kriterien:

- a) Kritikalität oder Bedeutung der Funktion und ihre möglichen Auswirkungen auf den Finanzsektor und die Finanzstabilität auf Unions- und nationaler Ebene,
- b) Bedeutung der Funktion für den laufenden Geschäftsbetrieb des Finanzunternehmens,
- c) Austauschbarkeit der Funktion,
- d) Verflechtung mit anderen Funktionen,
- e) geografischer Standort der Funktion,
- f) sektorale Abhängigkeit anderer Unternehmen von der Funktion,
- g) Bedrohungsanalysen in Bezug auf die Funktion, soweit vorhanden.

(8) Das Kontrollteam legt die Informationen über die Einleitung des TLPT und das Scoping-Dokument den Testern und Anbietern von Bedrohungsanalysen vor, sobald diese beauftragt wurden. Das Kontrollteam informiert die Tester und Anbieter von Bedrohungsanalysen über das anzuwendende Testverfahren.

(9) Das Finanzunternehmen stellt sicher, dass die Beauftragung oder Zuweisung von Testern und Anbietern von Bedrohungsanalysen vor Beginn der Testphase abgeschlossen ist.

(10) Vor Einleitung der Testphase konsultiert das Kontrollteam die Testmanager zur TLPT-bezogenen Risikobewertung und zu den Risikomanagementmaßnahmen. Das Kontrollteam überprüft die Risikobewertung bzw. die Risikomanagementmaßnahmen, wenn die TLPT-Behörde der Auffassung ist, dass sie den mit dem TLPT verbundenen Risiken nicht angemessen Rechnung tragen.

(11) Das Kontrollteam bewertet die Einhaltung der Anforderungen des Artikels 27 der Verordnung (EU) 2022/2554 und des Artikels 7 Absatz 1 der vorliegenden Verordnung durch die Anbieter von Bedrohungsanalysen und Tester, die es in den TLPT einbeziehen möchte, und dokumentiert das Ergebnis dieser Bewertung. Das Kontrollteam wählt die Anbieter von Bedrohungsanalysen nach Maßgabe dieser Bewertung und seiner Risikomanagementpraktiken aus. Vor der Beauftragung der ausgewählten Anbieter von Bedrohungsanalysen und externen Tester legt das Kontrollteam den Testmanagern Nachweise vor, dass diese Anbieter und Tester die Anforderungen des Artikels 27 der Verordnung (EU) 2022/2554 und des Artikels 7 Absatz 1 der vorliegenden Verordnung erfüllen. Das Kontrollteam darf die ausgewählten Anbieter von Bedrohungsanalysen und externen Tester nicht beauftragen, wenn die TLPT-Behörde der Auffassung ist, dass die ausgewählten Anbieter von Bedrohungsanalysen und externen Tester die Anforderungen des Artikels 27 der Verordnung (EU) 2022/2554 oder die in Artikel 7 Absatz 1 der vorliegenden Verordnung festgelegten Anforderungen oder zusätzliche Anforderungen, die sich aus einzelstaatlichen Rechtsvorschriften über die Sicherheit im Einklang mit dem Unionsrecht ergeben, nicht erfüllen, oder wenn das Finanzunternehmen die Anforderungen des Artikels 7 Absatz 2 Unterabsatz 1 der vorliegenden Verordnung nicht erfüllt oder wenn die in Artikel 7 Absatz 2 Unterabsatz 2 der vorliegenden Verordnung genannten Voraussetzungen nicht gegeben sind.

(12) Ist das Scoping-Dokument vollständig und gewährleistet die Durchführung eines angemessenen und wirksamen TLPT, so genehmigt die TLPT-Behörde dieses Dokument und unterrichtet den Leiter des Kontrollteams darüber.

*Artikel 10***Testphase: Bedrohungsanalyse**

(1) Nach Genehmigung des Scoping-Dokuments durch die TLPT-Behörde analysiert der Anbieter von Bedrohungsanalysen allgemeine und sektorspezifische Informationen über Bedrohungen, die für das Finanzunternehmen relevant sind. Hat die TLPT-Behörde für den Finanzsektor eines Mitgliedstaats Informationen über die allgemeine Bedrohungslage bereitgestellt, so kann der Anbieter von Bedrohungsanalysen diese Informationen als Grundlage für die nationale Bedrohungslage verwenden. Der Anbieter von Bedrohungsanalysen ermittelt Cyberbedrohungen sowie bestehende oder potenzielle Schwachstellen in Bezug auf das Finanzunternehmen. Darüber hinaus sammelt der Anbieter von Bedrohungsanalysen Informationen über das Finanzunternehmen und analysiert konkrete, verwertbare und kontextbezogene Informationen zu möglichen Angriffszielen und Bedrohungen betreffend das Finanzunternehmen, unter anderem durch Konsultation des Kontrollteams und der Testmanager.

(2) Der Anbieter von Bedrohungsanalysen legt dem Kontrollteam, den Testern und den Testmanagern die relevanten Bedrohungen und spezifische Bedrohungsinformationen dar und schlägt die erforderlichen Szenarien vor. Die vorgeschlagenen Szenarien sollen sich abhängig von den ermittelten Angriffen und den entsprechenden Taktiken, Techniken und Verfahren unterscheiden und auf jede kritische oder wichtige Funktion im Anwendungsbereich des TLPT abzielen.

(3) Der Leiter des Kontrollteams wählt mindestens drei Szenarien für die Durchführung des TLPT aus und berücksichtigt dabei alle folgenden Elemente:

- a) Empfehlung des Anbieters von Bedrohungsanalysen und bedrohungsorientierter Charakter jedes Szenarios,
- b) Beiträge der Testmanager,
- c) Durchführbarkeit der vorgeschlagenen Szenarien auf der Grundlage der Experteneinschätzung der Tester,
- d) Größe, Komplexität und Gesamtrisikoprofil des Finanzunternehmens sowie Art, Umfang und Komplexität seiner Dienstleistungen, Tätigkeiten und Geschäftsprozesse.

(4) Höchstens eines der ausgewählten Szenarien darf nicht bedrohungsorientiert sein und kann auf einer zukunftsorientierten und potenziell fiktiven Bedrohung mit hohem prädiktivem, antizipativem, opportunistischem oder prospektivem Wert angesichts der erwarteten Entwicklungen der Bedrohungslage für das Finanzunternehmen beruhen.

Bei gebündelten TLPT umfasst unbeschadet der Szenarien, die direkt auf die kritischen oder wichtigen Funktionen der an dem Test beteiligten Finanzunternehmen ausgerichtet sind, mindestens ein Szenario die einschlägigen zugrunde liegenden IKT-Systeme, -Prozesse und -Technologien des IKT-Drittdienstleisters, die die kritischen oder wichtigen Funktionen der in den Anwendungsbereich fallenden Finanzunternehmen unterstützen.

Handelt es sich bei dem Test um einen gemeinsamen TLPT, an dem ein gruppeninterner IKT-Dienstleister beteiligt ist, umfasst unbeschadet der Szenarien, die direkt auf die kritischen oder wichtigen Funktionen der an dem Test beteiligten Finanzunternehmen ausgerichtet sind, mindestens ein Szenario die einschlägigen zugrunde liegenden IKT-Systeme, -Prozesse und -Technologien des gruppeninternen IKT-Dienstleisters, die die kritischen oder wichtigen Funktionen der in den Anwendungsbereich fallenden Finanzunternehmen unterstützen.

(5) Bedrohungsanalysebericht, in dem die gemäß den Absätzen 3 und 4 ausgewählten Szenarien berücksichtigt sind. Der Bedrohungsanalysebericht enthält die in Anhang III aufgeführten Informationen.

(6) Das Kontrollteam legt dem Testmanager den spezifischen Bedrohungsanalysebericht zur Genehmigung vor. Ist der spezifische Bedrohungsanalysebericht vollständig und gewährleistet die Durchführung eines wirksamen TLPT, so genehmigt die TLPT-Behörde diesen Bericht und unterrichtet den Leiter des Kontrollteams darüber.

*Artikel 11***Testphase: Red-Team-Test**

(1) Nach Genehmigung des spezifischen Bedrohungsanalyseberichts durch die TLPT-Behörde arbeiten die Tester den Red-Team-Testplan aus, der die in Anhang IV aufgeführten Informationen enthält. Die Tester verwenden als Grundlage für die Entwicklung der Angriffsszenarien das Scoping-Dokument und den spezifischen Bedrohungsanalysebericht.

(2) Die Tester konsultieren das Kontrollteam, den Anbieter von Bedrohungsanalysen und die Testmanager zu dem Red-Team-Testplan, einschließlich der Kommunikations-, Verfahrens- und Projektmanagementmodalitäten, der vorbereitenden Maßnahmen und Anwendungsfälle für die Aktivierung der Hilfestellungen sowie der Modalitäten für die Berichterstattung an das Kontrollteam und die Testmanager.

(3) Ist der Red-Team-Testplan vollständig und gewährleistet die Durchführung eines wirksamen TLPT, so genehmigen das Kontrollteam und die TLPT-Behörde den Plan und die TLPT-Behörde unterrichtet den Leiter des Kontrollteams darüber.

(4) Nach Genehmigung des Red-Team-Testplans gemäß Absatz 3 führen die Tester den TLPT während der aktiven Red-Team-Testphase durch.

(5) Die Dauer der aktiven Red-Team-Testphase steht in einem angemessenen Verhältnis zum Umfang des TLPT sowie zur Größe, Tätigkeit, Komplexität und Anzahl der am TLPT beteiligten Finanzunternehmen und IKT-Drittdienstleister oder gruppeninternen IKT-Dienstleister und beträgt in jedem Fall mindestens zwölf Wochen. Angriffsszenarien können nacheinander oder gleichzeitig durchgeführt werden. Das Kontrollteam, der Anbieter von Bedrohungsanalysen, die Tester und die Testmanager einigen sich auf das Ende der aktiven Red-Team-Testphase.

(6) Sofern die Vollständigkeit des Red-Team-Testplans weiterhin gewährleistet ist und die Durchführung eines wirksamen TLPT möglich ist, genehmigen der Leiter des Kontrollteams und die Testmanager etwaige Änderungen des Red-Team-Testplans nach dessen Genehmigung, die sich auf den Zeitplan, den Umfang, die anzugreifenden Ziele oder die Flags beziehen können.

(7) Während der gesamten aktiven Red-Team-Testphase erstatten die Tester dem Kontrollteam und den Testmanagern mindestens wöchentlich über den Fortgang des TLPT Bericht, und der Anbieter von Bedrohungsanalysen steht dem Kontrollteam auf Anfrage für Konsultationen und zusätzliche Bedrohungsanalysen zur Verfügung.

(8) Das Kontrollteam leistet rechtzeitig die auf der Grundlage des Red-Team-Testplans ausgearbeiteten Hilfestellungen. Nach Genehmigung durch das Kontrollteam und die Testmanager können Hilfestellungen hinzugefügt oder angepasst werden.

(9) Werden die Testaktivitäten von einem Mitarbeiter des Finanzunternehmens oder gegebenenfalls seines IKT-Drittdienstleisters oder eines gruppeninternen IKT-Dienstleisters aufgedeckt, so schlägt das Kontrollteam den Testmanagern in Absprache mit den Testern und unbeschadet des Absatzes 10 Maßnahmen vor, die es ermöglichen, den TLPT fortzusetzen und gleichzeitig die Geheimhaltung zu wahren; diese Vorschläge werden von den Testmanagern validiert.

(10) Unter außergewöhnlichen Umständen, die das Risiko von Auswirkungen auf Daten, Schäden an Vermögenswerten und Störungen kritischer oder wichtiger Funktionen, Dienste oder Tätigkeiten des Finanzunternehmens selbst, seiner IKT-Drittdienstleister oder gruppeninternen IKT-Dienstleister oder Störungen bei seinen Gegenparteien oder im Finanzsektor hervorrufen, kann der Leiter des Kontrollteams den TLPT aussetzen oder als letztes Mittel, wenn die Fortsetzung des TLPT nicht anderweitig möglich ist und vorbehaltlich der vorherigen Validierung durch die TLPT-Behörde, den TLPT mit einer begrenzten Purple-Teaming-Übung fortführen. Die Dauer der begrenzten Purple-Teaming-Übung wird auf die Mindestdauer der aktiven Red-Team-Testphase von zwölf Wochen gemäß Absatz 5 angerechnet.

*Artikel 12***Abschlussphase**

- (1) Nach dem Ende der aktiven Red-Team-Testphase teilt der Leiter des Kontrollteams dem Blue Team mit, dass ein TLPT stattgefunden hat.
- (2) Innerhalb von vier Wochen nach dem Ende der aktiven Red-Team-Testphase legen die Tester dem Kontrollteam einen Red-Team-Testbericht vor, der die in Anhang V aufgeführten Informationen enthält.
- (3) Das Kontrollteam legt den Red-Team-Testbericht umgehend dem Blue Team und den Testmanagern vor.

Sofern von den Testmanagern verlangt, darf der in Unterabsatz 1 genannte Bericht keine sensiblen Informationen enthalten.

- (4) Nach Eingang des Red-Team-Testberichts, spätestens jedoch zehn Wochen nach dem Ende der aktiven Red-Team-Testphase, legt das Blue Team dem Kontrollteam einen Blue-Team-Testbericht vor, der die in Anhang VI aufgeführten Informationen enthält. Das Kontrollteam legt den Blue-Team-Testbericht umgehend den Testern und den Testmanagern vor.

Sofern von den Testmanagern verlangt, darf der in Unterabsatz 1 genannte Bericht keine sensiblen Informationen enthalten.

- (5) Spätestens zehn Wochen nach dem Ende der aktiven Red-Team-Testphase wiederholen das Blue Team und die Tester die während des TLPT vorgenommenen offensiven und defensiven Handlungen. Das Kontrollteam führt zudem Purple-Teaming-Übungen zu Themen durch, die vom Blue Team und den Testern gemeinsam auf der Grundlage der während des Tests festgestellten Schwachstellen ermittelt wurden, und gegebenenfalls zu Fragen, die während der aktiven Red-Team-Testphase nicht getestet werden konnten.

- (6) Nach Abschluss der Wiederholungsaktivitäten und der Purple-Teaming-Übungen geben das Kontrollteam, das Blue Team, die Tester und die Anbieter von Bedrohungsanalysen einander Rückmeldungen zu dem TLPT-Verfahren. Die Testmanager können Rückmeldungen geben.

- (7) Sobald die TLPT-Behörde den Leiter des Kontrollteams darüber unterrichtet hat, dass der Blue-Team-Testbericht und der Red-Team-Testbericht ihrer Bewertung zufolge die in den Anhängen V und VI aufgeführten Informationen enthalten, legt das Finanzunternehmen der TLPT-Behörde gemäß Artikel 26 Absatz 6 der Verordnung (EU) 2022/2554 innerhalb von acht Wochen den Bericht mit einer Zusammenfassung der maßgeblichen Ergebnisse des TLPT, der die in Anhang VII aufgeführten Angaben enthält, zur Genehmigung vor.

Sofern von der TLPT-Behörde verlangt, darf der in Unterabsatz 1 genannte Bericht keine sensiblen Informationen enthalten.

*Artikel 13***Plan mit Abhilfemaßnahmen**

- (1) Innerhalb von acht Wochen nach der in Artikel 12 Absatz 7 der vorliegenden Verordnung genannten Unterrichtung legt das Finanzunternehmen der TLPT-Behörde und — sofern es sich nicht um dieselbe Behörde handelt — der für das Finanzunternehmen zuständigen Behörde die in Artikel 26 Absatz 6 der Verordnung (EU) 2022/2554 genannten Pläne mit Abhilfemaßnahmen und Dokumente vor.

- (2) Der in Absatz 1 genannte Plan mit Abhilfemaßnahmen enthält für jedes Ergebnis im Rahmen des TLPT Folgendes:

- a) Beschreibung der festgestellten Mängel,
- b) Beschreibung der vorgeschlagenen Abhilfemaßnahmen, ihrer Priorisierung und ihres voraussichtlichen Abschlusses, gegebenenfalls einschließlich Maßnahmen zur Verbesserung der Identifizierungs-, Schutz-, Erkennungs- und Reaktionsfähigkeiten,
- c) Ursachenanalyse,
- d) Mitarbeiter oder Funktionen des Finanzunternehmens, die für die Umsetzung der vorgeschlagenen Abhilfemaßnahmen oder Verbesserungen verantwortlich sind,
- e) Risiken in Verbindung mit einer ausbleibenden Umsetzung der unter Buchstabe b genannten Maßnahmen und gegebenenfalls die mit der Umsetzung dieser Maßnahmen verbundenen Risiken.

*Artikel 14***Bescheinigung**

- (1) Die in Artikel 26 Absatz 7 der Verordnung (EU) 2022/2554 genannte Bescheinigung muss die in Anhang VIII aufgeführten Angaben enthalten.
- (2) Wenn mehrere TLPT-Behörden an einem TLPT beteiligt waren, stellt die federführende TLPT-Behörde den getesteten Finanzunternehmen die in Artikel 26 Absatz 7 der Verordnung (EU) 2022/2554 genannte Bescheinigung aus.

*Artikel 15***Einsatz interner Tester**

- (1) Die Finanzunternehmen treffen alle folgenden Vorkehrungen für den Einsatz interner Tester:
- a) Festlegung und Umsetzung einer Strategie für das Management interner Tester bei einem TLPT,
  - b) Maßnahmen, mit denen sichergestellt wird, dass sich der Einsatz interner Tester für die Durchführung eines TLPT nicht nachteilig auf die allgemeinen Verteidigungs- oder Resilienzfähigkeiten des Finanzunternehmens in Bezug auf IKT-bezogene Vorfälle auswirkt oder sich erheblich auf die Verfügbarkeit von Ressourcen auswirkt, die während eines TLPT für IKT-bezogene Aufgaben eingesetzt werden,
  - c) Maßnahmen, mit denen sichergestellt wird, dass interne Tester über ausreichende Ressourcen und Fähigkeiten verfügen, um einen TLPT durchzuführen.

Die unter Buchstabe a genannte Strategie muss

- a) Kriterien für die Beurteilung von Eignung, Kompetenz und potenziellen Interessenkonflikten der internen Tester enthalten und die Zuständigkeiten der Geschäftsleitung in dem Testverfahren enthalten,
- b) dokumentiert und regelmäßig überprüft werden,
- c) vorsehen, dass dem internen Testteam ein Testmanager und mindestens zwei zusätzliche Mitglieder angehören,
- d) verlangen, dass alle Mitglieder des Testteams in den vorangegangenen zwölf Monaten bei dem Finanzunternehmen oder einem gruppeninternen IKT-Dienstleister beschäftigt waren,
- e) Schulungen zur Durchführung von Penetrationstests und Red-Team-Tests für die internen Tester vorsehen.

(2) Wenn eine TLPT-Behörde den Einsatz interner Tester gemäß Artikel 27 Absatz 2 Buchstabe a der Verordnung (EU) 2022/2554 genehmigt, berücksichtigt die TLPT-Behörde die in Artikel 7 Absatz 1 der vorliegenden Verordnung festgelegten Anforderungen.

(3) Beim Einsatz interner Tester stellt das Finanzunternehmen sicher, dass in den folgenden Dokumenten darauf verwiesen wird:

- a) Informationen über die Einleitung des Tests gemäß Artikel 9,
- b) Red-Team-Testbericht gemäß Artikel 12 Absatz 2,
- c) Bericht mit einer Zusammenfassung der maßgeblichen Ergebnisse des TLPT gemäß den Artikeln 26 Absatz 6 der Verordnung (EU) 2022/2554.

(4) Tester, die bei einem gruppeninternen IKT-Dienstleister beschäftigt sind, gelten als interne Tester des Finanzunternehmens.

## Artikel 16

**Zusammenarbeit und gegenseitige Anerkennung**

- (1) Für die Durchführung eines TLPT bei einem Finanzunternehmen, das Dienstleistungen in mehr als einem Mitgliedstaat, auch über eine Zweigniederlassung, erbringt, muss die jeweils zuständige TLPT-Behörde
- a) bestimmen, welche TLPT-Behörden in den Aufnahmemitgliedstaaten beteiligt werden sollen; dabei ist zu berücksichtigen, ob eine oder mehrere kritische oder wichtige Funktionen in den Aufnahmemitgliedstaaten ausgeübt oder von diesen gemeinsam genutzt werden,
  - b) die gemäß Buchstabe a bestimmten TLPT-Behörden über die Entscheidung, einen TLPT bei dem Finanzunternehmen durchzuführen, unterrichten,
  - c) die Leitung des TLPT übernehmen, sofern die TLPT-Behörden nichts anderes vereinbaren.

Die TLPT-Behörden der Aufnahmemitgliedstaaten können innerhalb von zwanzig Arbeitstagen nach Erhalt der Informationen über die künftige Durchführung eines TLPT entweder ihr Interesse daran bekunden, den TLPT als Beobachter zu verfolgen, oder einen Testmanager benennen, der an dem TLPT teilnimmt. Die federführende TLPT-Behörde übermittelt allen TLPT-Behörden, die als Beobachter an dem TLPT teilnehmen, das Scoping-Dokument, den zusammenfassenden Testbericht, den Plan mit Abhilfemaßnahmen und die Bescheinigung.

Die federführende TLPT-Behörde koordiniert alle teilnehmenden TLPT-Behörden während des gesamten Tests und trifft alle Entscheidungen, die für eine angemessene und wirksame Durchführung des TLPT erforderlich sind. Die federführende TLPT-Behörde kann festlegen, dass die Zahl der teilnehmenden TLPT-Behörden eine bestimmte Schwelle nicht übersteigen darf, wenn andernfalls die wirksame Durchführung des TLPT gefährdet werden könnte.

(2) Nimmt ein Finanzunternehmen denselben gruppeninternen IKT-Dienstleister in Anspruch wie Finanzunternehmen mit Sitz in anderen Mitgliedstaaten oder gehört es einer Gruppe an und nutzt IKT-Systeme gemeinsam mit Finanzunternehmen derselben Gruppe, die in anderen Mitgliedstaaten niedergelassen sind, so wendet sich die für das Finanzunternehmen zuständige TLPT-Behörde an die für die anderen Finanzunternehmen zuständigen TLPT-Behörden, die dieselben gruppeninternen IKT-Dienstleister in Anspruch nehmen oder IKT-Systeme als Teil der Gruppe gemeinsam nutzen, und bewertet gemeinsam mit diesen die Durchführbarkeit und Eignung eines gemeinsamen TLPT. Ein gemeinsamer TLPT ist einem Einzel-TLPT vorzuziehen, wenn dadurch bei den Finanzunternehmen und den TLPT-Behörden Kosten gesenkt und Ressourcen eingespart werden können, sofern die Belastbarkeit und Wirksamkeit der Tests nicht beeinträchtigt werden.

- (3) Für die Durchführung eines gemeinsamen TLPT gilt Folgendes:
- a) Die für die Finanzunternehmen zuständigen TLPT-Behörden vereinbaren unter Berücksichtigung der Gruppenstruktur und der Wirksamkeit des Tests, welches Finanzunternehmen für die Durchführung des TLPT benannt wird.
  - b) Die für das gemäß Buchstabe a benannte Finanzunternehmen zuständige TLPT-Behörde leitet den TLPT, sofern die für die am gemeinsamen TLPT beteiligten Finanzunternehmen zuständigen TLPT-Behörden nichts anderes vereinbaren.
  - c) Die für die Finanzunternehmen, bei denen es sich nicht um das benannte Finanzunternehmen handelt, das den gemeinsamen TLPT leitet, zuständigen TLPT-Behörden können entweder ihr Interesse daran bekunden, den TLPT als Beobachter zu verfolgen, oder einen Testmanager für den betreffenden TLPT benennen.

Die federführende TLPT-Behörde koordiniert alle am gemeinsamen TLPT beteiligten TLPT-Behörden und trifft alle Entscheidungen, die für eine belastbare und wirksame Durchführung des gemeinsamen TLPT erforderlich sind.

(4) Beabsichtigt ein Finanzunternehmen, einen gebündelten TLPT gemäß Artikel 26 Absatz 4 der Verordnung (EU) 2022/2554 durchzuführen, an dem möglicherweise in anderen Mitgliedstaaten niedergelassene Finanzunternehmen beteiligt sind, so setzt sich seine TLPT-Behörde mit den für die anderen Finanzunternehmen zuständigen TLPT-Behörden in Verbindung und bewertet mit ihnen die Durchführbarkeit und Eignung eines gebündelten TLPT bei diesen Unternehmen gemäß Artikel 26 Absatz 4 der Verordnung (EU) 2022/2554.

- (5) Für die Durchführung eines gebündelten TLPT gemäß Artikel 26 Absatz 4 der Verordnung (EU) 2022/2554
- 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,
  - b) übernimmt die für das gemäß Buchstabe a benannte Finanzunternehmen zuständige TLPT-Behörde die Leitung für den TLPT, sofern die für die am gebündelten TLPT beteiligten Finanzunternehmen zuständigen TLPT-Behörden nichts anderes vereinbaren,
  - c) können die für die Finanzunternehmen, bei denen es sich nicht um das benannte Finanzunternehmen handelt, das den gemeinsamen TLPT leitet, zuständigen TLPT-Behörden entweder ihr Interesse daran bekunden, den TLPT als Beobachter zu verfolgen, oder einen Testmanager für den betreffenden TLPT benennen.

Die federführende TLPT-Behörde koordiniert alle am gebündelten TLPT beteiligten TLPT-Behörden und trifft alle Entscheidungen, die für eine belastbare und wirksame Durchführung des gebündelten TLPT erforderlich sind.

(6) Unterscheidet sich die für ein Finanzunternehmen, das einen TLPT durchführen muss, zuständige TLPT-Behörde von der in Artikel 46 der Verordnung (EU) 2022/2554 genannten zuständigen Behörde, so teilen diese Behörden alle relevanten Informationen über alle mit dem TLPT verbundenen Angelegenheiten für die Zwecke der Durchführung des TLPT oder zur Wahrnehmung ihrer Aufgaben gemäß der genannten Verordnung mit.

#### *Artikel 17*

#### **Inkrafttreten**

Diese Verordnung tritt am zwanzigsten Tag nach ihrer Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.

Diese Verordnung ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat.

Brüssel, den 13. Februar 2025

*Für die Kommission*  
*Die Präsidentin*  
Ursula VON DER LEYEN

## ANHANG I

**Inhalt der Projektcharta (Artikel 9 Absatz 2 Buchstabe a)**

Information	Erforderliche Angaben
Für den Projektplan verantwortliche Person, d. h. Leiter des Kontrollteams	Name Kontaktdaten
Tester	<input type="checkbox"/> intern <input type="checkbox"/> extern <input type="checkbox"/> beides
Gemäß Artikel 9 Absatz 2 Buchstabe d und Artikel 9 Absatz 4 Buchstabe a gewählte Kommunikationskanäle, einschließlich: a) Verwendung von E-Mail-Verschlüsselung b) Verwendung von Online-Datenräumen c) Verwendung von Instant Messaging	
Codename des TLPT	
Etwaige kritische oder wichtige Funktionen, die das Finanzunternehmen in anderen Mitgliedstaaten ausübt	1. Auflistung kritischer oder wichtiger Funktionen, die in einem anderen Mitgliedstaat ausgeübt werden 2. für jede kritische oder wichtige Funktion Angabe des Mitgliedstaats bzw. der Mitgliedstaaten, in dem (denen) sie ausgeübt werden
Etwaige kritische oder wichtige Funktionen, die von IKT-Drittdienstleistern unterstützt werden	3. Auflistung kritischer oder wichtiger Funktionen, die von IKT-Drittdienstleistern unterstützt werden 4. für jede Funktion Angabe des IKT-Drittdienstleisters
<i>Voraussichtliche Fristen für den Abschluss</i>	
1. der Vorbereitungsphase gemäß Artikel 9	JJJJ-MM-TT
2. der Testphase gemäß den Artikeln 10 und 11	JJJJ-MM-TT
3. der Abschlussphase gemäß Artikel 12	JJJJ-MM-TT
4. der Erstellung des Plans mit Abhilfemaßnahmen gemäß Artikel 13	JJJJ-MM-TT

## ANHANG II

**Inhalt des Scoping-Dokuments (Artikel 9 Absatz 6)**

1. Das Scoping-Dokument enthält eine Auflistung aller kritischen oder wichtigen Funktionen, die das Finanzunternehmen ermittelt hat.
2. Für jede ermittelte kritische oder wichtige Funktion sind folgende Angaben zu machen:
  - a) Wenn die kritische oder wichtige Funktion nicht in den Anwendungsbereich des TLPT fällt, Erläuterung der Gründe, aus denen sie nicht einbezogen wurde.
  - b) Wenn die kritische oder wichtige Funktion in den Anwendungsbereich des TLPT fällt:
    - i) Angabe der Gründe für die Einbeziehung,
    - ii) das (die) identifizierte(n) IKT-System(e) zur Unterstützung dieser kritischen oder wichtigen Funktion,
    - iii) für jedes ermittelte IKT-System:
      1. Angabe, ob es ausgelagert ist, und falls ja, Name des IKT-Drittdienstleisters,
      2. Rechtsräume, in denen das IKT-System verwendet wird,
      3. übergeordnete Beschreibung der vorläufigen Flags, aus der hervorgeht, welcher Sicherheitsaspekt (Vertraulichkeit, Integrität, Authentizität oder Verfügbarkeit) von dem einzelnen Flag erfasst ist.

---

## ANHANG III

**Inhalt des spezifischen Bedrohungsanalyseberichts (Artikel 10 Absatz 5)**

Der spezifische Bedrohungsanalysebericht enthält Informationen zu allen folgenden Punkten:

1. Gesamtumfang der Bedrohungsuntersuchungen, die mindestens Folgendes einbeziehen:
  - a) kritische oder wichtige Funktionen, die in den Anwendungsbereich fallen,
  - b) ihr geografischer Standort,
  - c) verwendete EU-Amtssprache,
  - d) relevante IKT-Drittdienstleister,
  - e) Zeitraum, in dem die Untersuchungen durchgeführt wurden.
2. Gesamtbewertung, welche konkreten verwertbaren Informationen über das Finanzunternehmen zu finden sind, unter anderem:
  - a) Benutzernamen und Passwörter der Mitarbeiter,
  - b) Look-Alike-Domains, die mit offiziellen Domains des Finanzunternehmens verwechselt werden können,
  - c) technische Auskundschaftung: (für Exploits) anfällige Software, Systeme und Technologien,
  - d) von Mitarbeitern im Internet veröffentlichte Informationen über das Finanzunternehmen, die für die Zwecke eines Angriffs verwendet werden könnten,
  - e) Informationen, die im Dark Web verkauft werden,
  - f) sonstige einschlägige Informationen, die im Internet oder in öffentlichen Netzwerken verfügbar sind,
  - g) gegebenenfalls Informationen über Möglichkeiten des physischen Zugangs, z. B. zu den Räumlichkeiten des Finanzunternehmens.
3. Bedrohungsanalysen unter Berücksichtigung der allgemeinen Bedrohungslage und der besonderen Situation des Finanzunternehmens, darunter mindestens:
  - a) das geopolitische Umfeld,
  - b) das wirtschaftliche Umfeld,
  - c) technologische und sonstige Trends im Zusammenhang mit den Tätigkeiten im Finanzdienstleistungssektor.
4. Bedrohungsprofile der böswilligen Akteure (bestimmte Einzelperson/Gruppe oder allgemeine Gruppe), die das Finanzunternehmen angreifen könnten, einschließlich der Systeme des Finanzunternehmens, die von böswilligen Akteuren am wahrscheinlichsten kompromittiert oder angegriffen werden, der möglichen Motivation, Absicht und Gründe für den möglichen zielgerichteten Angriff und der möglichen Vorgehensweise der Angreifer.
5. Bedrohungsszenarien: mindestens drei End-to-End-Bedrohungsszenarien für die gemäß Nummer 4 ermittelten Bedrohungsprofile, die die höchsten Werte für die Schwere der Bedrohung aufweisen. Die Bedrohungsszenarien beschreiben den End-to-End-Angriffspfad und umfassen mindestens:
  - a) ein Szenario, das u. a. eine Kompromittierung der Dienstverfügbarkeit umfasst,
  - b) ein Szenario, das u. a. eine Kompromittierung der Datenintegrität umfasst,
  - c) ein Szenario, das u. a. die Kompromittierung der Vertraulichkeit von Informationen umfasst.
6. Gegebenenfalls eine Beschreibung des in Artikel 10 Absatz 4 genannten nicht bedrohungsorientierten Szenarios.

## ANHANG IV

**Inhalt des Red-Team-Testplans (Artikel 11 Absatz 1)**

Der Red-Team-Testplan enthält Informationen zu allen folgenden Punkten:

- a) Kommunikationskanäle und -verfahren,
- b) für den Angriff zulässige und nicht zulässige Taktiken, Techniken und Verfahren, einschließlich ethischer Grenzen für Social Engineering,
- c) von den Testern zu ergreifende Risikomanagementmaßnahmen,
- d) Beschreibung jedes Szenarios, einschließlich
  - i) des simulierten Angreifers,
  - ii) seiner Absicht, Motivation und Ziele,
  - iii) der Funktionen und der unterstützenden IKT-Systeme, gegen die sich der Angriff richtet,
  - iv) der Aspekte der Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität, auf die der Angriff ausgerichtet ist,
  - v) Flags,
- e) detaillierte Beschreibung jedes voraussichtlichen Angriffspfads, einschließlich der Voraussetzungen und etwaigen Hilfestellungen durch das Kontrollteam, mit Angabe der zeitlichen Vorgaben für deren Aktivierung und potenziellen Verwendung,
- f) Planung der Red-Teaming-Aktivitäten, einschließlich der Zeitplanung für die Durchführung jedes Szenarios, mindestens aufgeschlüsselt nach den drei Phasen, die ein Tester während der Testphase absolviert, d. h. Eindringen in die IKT-Systeme des Finanzunternehmens, Bewegung durch die IKT-Systeme und letztlich Erreichen des Angriffsziels und Rückzug aus den IKT-Systemen (In-, Through- und Out-Phase),
- g) Besonderheiten der Infrastruktur der Finanzunternehmen, die bei den Tests zu berücksichtigen sind,
- h) gegebenenfalls zusätzliche Informationen oder sonstige Ressourcen, die die Tester für die Ausführung der Szenarien benötigen.

---

## ANHANG V

**Inhalt des Red-Team-Testberichts (Artikel 12 Absatz 2)**

Der Red-Team-Testbericht enthält mindestens Informationen zu allen folgenden Punkten:

- a) Informationen über den durchgeführten Angriff, einschließlich Angaben zu
  - i) den angegriffenen kritischen oder wichtigen Funktionen und ermittelten IKT-Systemen, -Prozessen und -Technologien, die die kritische oder wichtige Funktion unterstützen, wie im Red-Team-Testplan festgelegt,
  - ii) Zusammenfassung jedes Szenarios,
  - iii) erreichte und nicht erreichte Flags,
  - iv) erfolgreich und nicht erfolgreich verfolgte Angriffspfade,
  - v) erfolgreich und nicht erfolgreich angewandte Taktiken, Techniken und Verfahren,
  - vi) etwaige Abweichungen vom Red-Team-Testplan,
  - vii) etwaige Hilfestellungen,
- b) alle Aktivitäten, von denen die Tester wissen, dass sie vom Blue Team durchgeführt wurden, um den Angriff zu rekonstruieren und seine Auswirkungen abzumildern,
- c) festgestellte Schwachstellen und andere Probleme, einschließlich:
  - i) Beschreibung der Schwachstelle und anderer Probleme, einschließlich ihrer Kritikalität,
  - ii) Ursachenanalyse erfolgreicher Angriffe,
  - iii) Empfehlungen für Abhilfemaßnahmen mit Priorisierung.

---

## ANHANG VI

**Inhalt des Blue-Team-Testberichts (Artikel 12 Absatz 4)**

Der Blue-Team-Testbericht enthält mindestens Informationen zu allen folgenden Punkten:

1. Für jeden von den Testern im Red-Team-Testbericht beschriebenen Angriffsschritt:
  - a) Auflistung der entdeckten Angriffshandlungen,
  - b) Protokolleinträge für diese entdeckten Handlungen,
2. Bewertung der Ergebnisse und Empfehlungen der Tester,
3. vom Blue Team gesammelte Beweise für den Angriff durch die Tester,
4. Blue-Team-Ursachenanalyse erfolgreicher Angriffe durch die Tester,
5. Auflistung der gewonnenen Erkenntnisse und ermittelten Verbesserungspotenziale,
6. Auflistung der Themen, die beim Purple-Teaming behandelt werden sollen.

---

## ANHANG VII

**Inhalt des Berichts mit einer Zusammenfassung der maßgeblichen Ergebnisse des TLPT gemäß Artikel 26 Absatz 6 der Verordnung (EU) 2022/2554**

Der zusammenfassende Testbericht muss mindestens Angaben zu allen folgenden Punkten enthalten:

- a) beteiligte Parteien,
- b) Projektplan,
- c) validierter Umfang, einschließlich der Gründe für die Einbeziehung oder den Ausschluss kritischer oder wichtiger Funktionen und ermittelter IKT-Systeme, -Prozesse und -Technologien, die die vom TLPT erfassten kritischen oder wichtigen Funktionen unterstützen,
- d) gewählte Szenarien und etwaige erhebliche Abweichungen vom spezifischen Bedrohungsanalysebericht,
- e) verfolgte Angriffspfade und angewandte Taktiken, Techniken und Verfahren,
- f) erreichte und nicht erreichte Flags,
- g) etwaige Abweichungen vom Red-Team-Testplan,
- h) etwaige vom Blue Team aufgedeckte Handlungen,
- i) Purple-Teaming in der Testphase, sofern durchgeführt, und zugrunde liegende Voraussetzungen,
- j) etwaige Hilfestellungen,
- k) ergriffene Risikomanagementmaßnahmen,
- l) festgestellte Schwachstellen und andere Probleme, einschließlich ihrer Kritikalität,
- m) Ursachenanalyse erfolgreicher Angriffe,
- n) umfassender Plan mit Abhilfemaßnahmen, in dem Schwachstellen und andere festgestellte Probleme, ihre Ursachen und die Priorität der Behebung zueinander in Beziehung gesetzt werden,
- o) Erkenntnisgewinn aus den Rückmeldungen.

---

## ANHANG VIII

**Inhalt der Bescheinigung über den TLPT gemäß Artikel 26 Absatz 7 der Verordnung (EU) 2022/2554**

Die Bescheinigung enthält mindestens alle folgenden Angaben:

- a) Zum durchgeführten TLPT:
  - i) Beginn und Ende des TLPT,
  - ii) die kritischen oder wichtigen Funktionen, die Gegenstand des Tests waren,
  - iii) gegebenenfalls Informationen über kritische oder wichtige Funktionen, die Gegenstand des Tests waren und für die der TLPT nicht durchgeführt wurde,
  - iv) etwaige andere Finanzunternehmen, die an dem TLPT beteiligt waren,
  - v) etwaige IKT-Drittdienstleister, die an dem TLPT beteiligt waren,
  - vi) zu den Testern:
    - 1. Angabe, ob interne Tester eingesetzt wurden,
    - 2. Angabe, ob das Finanzunternehmen von Artikel 5 Absatz 3 Unterabsatz 2 Gebrauch gemacht hat,
  - vii) Dauer der aktiven Red-Team-Testphase in Kalendertagen,
- b) wenn mehrere TLPT-Behörden an dem TLPT beteiligt waren: Nennung der anderen TLPT-Behörden und Angabe, in welcher Eigenschaft sie daran beteiligt waren,
- c) Aufstellung der Dokumente, die von der TLPT-Behörde für die Ausstellung der Bescheinigung geprüft wurden.

---