Publicatieblad
van de Europese Unie

NL
L-serie

2025/1190

18.6.2025

GEDELEGEERDE VERORDENING (EU) 2025/1190 VAN DE COMMISSIE

van 13 februari 2025

tot aanvulling van Verordening (EU) 2022/2554 van het Europees Parlement en de Raad met technische reguleringsnormen tot nadere bepaling van de criteria voor het identificeren van financiële entiteiten die threat-led penetratietests moeten uitvoeren, de vereisten en normen inzake het inzetten van interne testers, de vereisten met betrekking tot de scope, testmethodologie en -aanpak voor elke fase van de tests, de resultaten, de afsluitende en de remediëringsfase, en het soort samenwerking op het gebied van toezicht en andere relevante vormen van samenwerking die noodzakelijk zijn voor de uitvoering van TLPT's en ter facilitering van wederzijdse erkenning van die tests

(Voor de EER relevante tekst)

DE EUROPESE COMMISSIE,

Gezien het Verdrag betreffende de werking van de Europese Unie,

Gezien Verordening (EU) 2022/2554 van het Europees Parlement en de Raad van 14 december 2022 betreffende digitale operationele weerbaarheid voor de financiële sector en tot wijziging van Verordeningen (EG) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 en (EU) 2016/1011 ([1]), en met name artikel 26, lid 11, vierde alinea,

Overwegende hetgeen volgt:

(1) Deze verordening is opgesteld overeenkomstig het TIBER-EU Framework en weerspiegelt de methodologie, het proces en de structuur van threat-led penetration tests ("TLPT's") zoals beschreven in TIBER-EU. Financiële entiteiten die TLPT moeten uitvoeren, kunnen verwijzen naar en toepassing geven aan het TIBER-EU Framework, of een van de nationale uitvoeringen ervan, voor zover dat raamwerk of die uitvoering in overeenstemming is met de vereisten van de artikelen 26 en 27 van Verordening (EU) 2022/2554 en met deze verordening. De aanwijzing van één enkele overheidsinstantie in de financiële sector die overeenkomstig artikel 26, lid 9, van Verordening (EU) 2022/2554 op nationaal niveau verantwoordelijk is voor TLPT-gerelateerde aangelegenheden, mag geen afbreuk doen aan de bevoegdheden van bevoegde autoriteiten die op Unieniveau zijn belast met het toezicht op bepaalde financiële entiteiten overeenkomstig artikel 46 van die verordening, zoals bijvoorbeeld aan de Europese Centrale Bank voor belangrijke kredietinstellingen, die moeten worden geacht bevoegd te zijn voor TLPT-kwesties. Indien alleen sommige van de TLPT-gerelateerde taken overeenkomstig artikel 26, lid 10, van Verordening (EU) 2022/2554 aan een andere nationale autoriteit in de financiële sector worden gedelegeerd, moet de in artikel 46 van die verordening bedoelde bevoegde autoriteit van de financiële entiteit de autoriteit blijven voor de TLPT-gerelateerde taken die niet gedelegeerd zijn.

(2) Gezien de complexiteit van TLPT's en de daaraan verbonden risico's, moet het gebruik van TLPT's worden beperkt tot financiële entiteiten waarvoor zulks gerechtvaardigd is. Daarom moeten de autoriteiten die verantwoordelijk zijn voor TLPT-aangelegenheden ("TLPT-autoriteiten", op het niveau van de Unie of op nationaal niveau), financiële entiteiten die actief zijn in subsectoren van financiële kerndiensten waarvoor een TLPT niet gerechtvaardigd is, uitsluiten van de scope van TLPT's. Dat betekent dat kredietinstellingen, betaalinstellingen en instellingen voor elektronisch geld, centrale effectenbewaarinstellingen, centrale tegenpartijen, handelsplatformen, (her)verzekeringsondernemingen, ook als zij aan de kwantitatieve criteria voldoen, van de verplichting om TLPT's uit te voeren kunnen worden vrijgesteld in het licht van een algemene beoordeling van hun ICT-risicoprofiel en -maturiteit, hun impact op de financiële sector en de daarmee samenhangende zorgen over de financiële stabiliteit.

(3) TLPT-autoriteiten moeten, in het licht van een algemene beoordeling van het ICT-risicoprofiel en de ICT-maturiteit, de impact op de financiële sector en de daarmee samenhangende zorgen over de financiële stabiliteit, beoordelen of andere soorten financiële entiteiten dan kredietinstellingen, betaalinstellingen, instellingen voor elektronisch geld, centrale tegenpartijen, centrale effectenbewaarinstellingen, handelsplatformen en (her)verzekeringsondernemingen aan TLPT's moeten worden onderworpen. De beoordeling of die financiële entiteiten voldoen aan voornoemde kwalitatieve criteria moet inzetten op het aan de hand van sectoroverschrijdende en objectieve indicatoren identificeren van de financiële entiteiten waarvoor TLPT's passend zijn. Tegelijkertijd moet die beoordeling of een financiële entiteit aan die kwalitatieve criteria voldoet, de aan TLPT's te onderwerpen entiteiten beperken tot die

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

entiteiten waarvoor zulks gerechtvaardigd is. De vraag of een financiële entiteit aan de kwalitatieve criteria voldoet, moet ook worden beantwoord in het licht van de nieuwe marktontwikkelingen en van het toenemende belang van nieuwe marktdeelnemers voor de financiële sector in de toekomst, met inbegrip van aanbieders van cryptoactiva-diensten die overeenkomstig artikel 59 van Verordening (EU) 2023/1114 van het Europees Parlement en de Raad ([2]) een vergunning hebben gekregen.

(4) Financiële entiteiten kunnen dezelfde intragroepsaanbieder van ICT-diensten hebben of kunnen tot dezelfde groep behoren en gebruikmaken van gedeelde ICT-systemen. In dat geval is het belangrijk dat TLPT-autoriteiten, wanneer zij beoordelen of een financiële entiteit aan TLPT's moet worden onderworpen, en of de TLPT moet worden uitgevoerd op entiteitsniveau of op groepsniveau (via een gezamenlijke TLPT), de structuur en het systemische karakter of het belang van die financiële entiteit voor de financiële sector op nationaal of Unieniveau in aanmerking nemen.

(5) Om een afspiegeling te zijn van het TIBER-EU Framework, moet in de testmethodologie een rol voor de volgende hoofddeelnemers opgenomen zijn: de financiële entiteit, met een *control team* (de tegenhanger van het TIBER-EU "control team") en een blue team (de tegenhanger van het TIBER-EU "blue team"), de TLPT-autoriteit, in de vorm van een TLPT-cyberteam (de tegenhanger van de TIBER-EU "TIBER cyberteams"), een aanbieder van dreigingsinformatie, en testers (waarbij de testers de tegenhangers van de TIBER-EU "red-team provider" zijn).

(6) Om ervoor te zorgen dat de TLPT kan profiteren van de ervaringen die zijn opgedaan in het kader van de uitvoering van TIBER-EU, en om de aan de uitvoering van TLPT's verbonden risico's te verminderen, moet ervoor worden gezorgd dat de verantwoordelijkheden van de TLPT-cyberteams die op het niveau van TLPT-autoriteiten worden opgericht, zo nauw mogelijk aansluiten bij die van de TIBER-EU-cyberteams. Daarom moeten de TLPT-cyberteams beschikken over testmanagers die verantwoordelijk zijn voor het overzien van individuele TLPT's en voor het plannen en coördineren van individuele tests. TLPT-cyberteams moeten fungeren als centraal aanspreekpunt voor communicatie met interne en externe stakeholders over de tests, voor het verzamelen en verwerken van feedback en lessons learned van eerder uitgevoerde tests, en voor het ondersteunen van financiële entiteiten die TLPT's ondergaan.

(7) Om de methodologie van het TIBER-EU Framework te weerspiegelen, moeten testmanagers over de benodigde vaardigheden en capaciteiten beschikken om adviezen te geven en testers te bevragen over hun voorstellen. De in het kader van het TIBER-EU Framework opgedane ervaringen hebben uitgewezen dat het waardevol is om aan elke test een team van ten minste twee testmanagers toe te wijzen. Om te weerspiegelen dat TLPT's bedoeld zijn als een mogelijkheid om te leren, en om de vertrouwelijkheid van de tests te waarborgen, worden TLPT-autoriteiten sterk aangemoedigd om, tenzij zij kampen met een gebrek aan middelen of deskundigheid, te bepalen dat testmanagers voor de duur van een TLPT geen toezichtwerkzaamheden mogen uitvoeren ten aanzien van de financiële entiteit die een TLPT ondergaat.

(8) Met het oog op de samenhang met het TIBER-EU Framework is het belangrijk dat de TLPT-autoriteit de testwerkzaamheden in elk van de fasen ervan nauwlettend volgt. Gezien de aard van het testen en de risico's die daaraan verbonden zijn, is het van fundamenteel belang dat de TLPT-autoriteit wordt betrokken bij elke specifieke testfase. In het bijzonder moet de TLPT-autoriteit worden geraadpleegd en moeten beoordelingen of besluiten van de financiële entiteiten die van invloed kunnen zijn op de doeltreffendheid van de test en een impact kunnen hebben op de aan de test verbonden risico's, door haar worden gevalideerd. De fundamentele stappen waar een specifieke rol van de TLPT-autoriteit noodzakelijk is, zijn onder meer het valideren van bepaalde essentiële documentatie met betrekking tot de tests, de selectie van aanbieders van dreigingsinformatie en testers, en maatregelen inzake risicomanagement. De rol van de TLPT-autoriteiten, met name voor valideringen, mag niet leiden tot een buitensporige last voor die autoriteiten en moet daarom beperkt blijven tot de documenten en besluiten die rechtstreeks van invloed kunnen zijn op het uitvoeren van de TLPT. Door actief deel te nemen aan elke testfase, kunnen de TLPT-autoriteiten op doeltreffende wijze beoordelen of de financiële entiteiten de toepasselijke vereisten naleven, hetgeen die autoriteiten in staat moet stellen de in artikel 26, lid 7, van Verordening (EU) 2022/2554 bedoelde attesten af te geven.

([2]) Verordening (EU) 2023/1114 van het Europees Parlement en de Raad van 31 mei 2023 betreffende cryptoactivamarkten en tot wijziging van Verordeningen (EU) nr. 1093/2010 en (EU) nr. 1095/2010 en Richtlijnen 2013/36/EU en (EU) 2019/1937 (PB L 150 van 9.6.2023, blz. 40, ELI: http://data.europa.eu/eli/reg/2023/1114/oj).

(9) Om ervoor te zorgen dat de omstandigheden van de tests realistisch zijn, is geheimhouding van TLPT's van het grootste belang. Om die reden moeten de testwerkzaamheden heimelijk plaatsvinden en moeten voorzorgsmaatregelen worden genomen om de TLPT's vertrouwelijk te houden, onder meer door zodanige codenamen te kiezen dat identificatie van de TLPT door derden wordt voorkomen. Indien personeelsleden die verantwoordelijk zijn voor de beveiliging van het financiële team, op de hoogte zijn van een geplande of lopende TLPT, zullen zij waarschijnlijk oplettender en alerter zijn dan in normale werkomstandigheden, hetgeen een vertekende uitkomst van de test zal opleveren. Personeelsleden van de financiële entiteit die geen deel uitmaken van het *control team*, mogen daarom alleen op de hoogte worden gesteld van geplande of lopende TLPT's als daarvoor overtuigende redenen bestaan en na voorafgaande toestemming van de testmanagers, onder meer om de geheimhouding van de test te waarborgen indien een lid van het blue team heeft ontdekt dat de test loopt.

(10) Zoals de in het TIBER-EU Framework opgedane ervaringen met het *control team* hebben uitgewezen, is de selectie van een geschikte leider van het *control team* (control team lead) onontbeerlijk voor de veilige uitvoering van TLPT's. De leider van het *control team* moet binnen de financiële entiteit kunnen beschikken over het benodigde mandaat om alle aspecten van de tests aan te sturen, zonder de vertrouwelijkheid ervan in het gedrang te brengen. Om dezelfde reden moeten de leden van het *control team* een grondige kennis hebben van de financiële entiteit en van de functie en strategische positionering van de leider van het *control team*, moeten zij over de vereiste senioriteit beschikken en moeten zij toegang hebben tot de raad van bestuur. Om het risico op compromittering van de TLPT te verkleinen, moet het *control team* zo klein mogelijk worden gehouden.

(11) Aan TLPT's zijn inherente risico's verbonden, aangezien kritieke functies worden getest in een live productieomgeving, met de kans op denial-of-service(DoS)-incidenten, onverwachte systeemcrashes, schade aan kritieke live productiesystemen of het verlies, de wijziging of openbaarmaking van data. Die risico's onderstrepen de noodzaak van maatregelen voor robuust risicomanagement. Om de TLPT tijdens de gehele duur ervan op een gecontroleerde manier te laten verlopen, is het van groot belang dat financiële entiteiten zich te allen tijde bewust zijn van de specifieke risico's die zich bij een TLPT voordoen en dat die risico's worden gemitigeerd. In dat verband kan, onverminderd de interne processen van de financiële entiteit en de verantwoordelijkheden en delegaties die reeds aan de leider van het *control team* zijn verleend, het verstrekken van informatie over maatregelen voor TLPT-risicomanagement of, in bepaalde gevallen, de goedkeuring van die maatregelen voor risicomanagement door het leidinggevend orgaan van de financiële entiteit zelf, passend zijn. Om doeltreffende en de best gekwalificeerde professionele diensten te kunnen leveren en die risico's te verminderen, is het ook van essentieel belang dat de testers en aanbieders van dreigingsinformatie (tezamen "de TLPT-aanbieders") beschikken over het hoogste niveau aan vaardigheden en deskundigheid en over passende ervaring op het gebied van dreigingsinformatie en TLPT's in de sector financiële diensten.

(12) Conventionele penetratietests bieden een gedetailleerde en nuttige beoordeling van technische en configuratiekwetsbaarheden, vaak van één enkel, afzonderlijk systeem of één enkele, afzonderlijke omgeving, maar anders dan informatiegestuurde red-teamtests beoordelen zij niet het volledige scenario van een gerichte aanval op een hele entiteit, met inbegrip van al haar medewerkers, processen en technologieën. Tijdens het selectieproces van de TLPT-aanbieders moeten financiële entiteiten zich er daarom van verzekeren dat die aanbieders beschikken over de vereiste vaardigheden om informatiegestuurde red-teamtests uit te voeren — en niet alleen penetratietests. Om die reden moeten omvattende criteria worden vastgesteld voor (interne en externe) testers en aanbieders van dreigingsinformatie (die altijd extern zijn). Wanneer de TLPT-aanbieders tot dezelfde onderneming behoren, moet het personeel dat aan een TLPT wordt toegewezen, op adequate wijze worden afgescheiden.

(13) In bepaalde uitzonderlijke omstandigheden kan zich de situatie voordoen dat financiële entiteiten geen TLPT-aanbieders kunnen inhuren die aan de omvattende criteria voldoen. Financiële entiteiten moeten daarom de mogelijkheid hebben om, wanneer zij aantonen dat dergelijke aanbieders van dreigingsinformatie niet beschikbaar zijn, personen in te zetten die niet aan alle criteria voldoen, mits zij de daaruit voortvloeiende aanvullende risico's naar behoren mitigeren en de TLPT-autoriteit al die criteria beoordeelt.

(14) Wanneer meerdere financiële entiteiten en meerdere TLPT-autoriteiten bij een TLPT betrokken zijn, moeten de rollen van alle partijen in het TLPT-proces worden gespecificeerd om de TLPT op de meest efficiënte en veilige wijze uit te voeren. Voor het uitvoeren van gepoolde tests zijn specifieke vereisten nodig om de rol van de aangewezen financiële entiteit te specificeren, in de zin dat deze verantwoordelijk is voor het verstrekken van alle benodigde documentatie aan de leidende TLPT-autoriteit en voor het monitoren van het testproces. De aangewezen financiële entiteit moet ook verantwoordelijk zijn voor de gemeenschappelijke aspecten van de beoordeling van het risicomanagement. Niettegenstaande de rol van de aangewezen financiële entiteit mag een en ander niets afdoen aan de verplichtingen van elke financiële entiteit die aan het gepoolde TLPT-proces deelneemt, tijdens de gepoolde test. Hetzelfde beginsel moet gelden voor de uitvoering van gezamenlijke TLPT's.

(15) Zoals de ervaring bij de uitvoering van het TIBER-EU Framework heeft geleerd, is het houden van fysieke of on-line vergaderingen met alle betrokken stakeholders (financiële entiteiten, autoriteiten, testers en aanbieders van dreigingsinformatie) de meest doelmatige manier om ervoor te zorgen dat de tests correct worden uitgevoerd. Daarom moeten in de verschillende fasen van het proces fysieke en on-line vergaderingen worden gehouden, en meer bepaald in de voorbereidingsfase, bij de start van de TLPT en om de scope ervan te bepalen; in de testfase, om het rapport inzake dreigingsinformatie en het testplan voor het red team definitief vast te leggen, en voor de wekelijkse updates, en in de afsluitende fase, bij de replay van acties van testers en het blue team, voor purple teaming en om feedback over de TLPT uit te wisselen.

(16) Om de TLPT soepel te laten verlopen, moet de TLPT-autoriteit haar verwachtingen met betrekking tot de test duidelijk presenteren aan de financiële entiteit. In dat verband moeten de testmanagers ervoor zorgen dat er een passende informatiestroom tot stand wordt gebracht met het *control team* binnen de financiële entiteit en met de TLPT-aanbieders.

(17) De financiële entiteit moet de in de scope van de TLPT op te nemen kritieke of belangrijke functies selecteren. Bij het selecteren van die functies moet de financiële entiteit zich baseren op verschillende criteria die verband houden met het belang van elke functie voor de financiële entiteit zelf en voor de financiële sector, op het niveau van de Unie en op nationaal niveau, niet alleen in economische zin, maar ook rekening houdende met de symbolische of politieke status van de functie. Om een soepele overgang naar de fase van het verzamelen van dreigingsinformatie te vergemakkelijken, moet het *control team* de testers en de aanbieder van dreigingsinformatie (threat intelligence provider) die niet bij de scoping betrokken zijn, gedetailleerde informatie over de overeengekomen scoping verstrekken.

(18) Om de testers te voorzien van de informatie die nodig is voor het simuleren van een levensechte en realistische aanval op de live systemen van de financiële entiteit die haar kritieke of belangrijke functies ondersteunen, moet de aanbieder van dreigingsinformatie inlichtingen of informatie verzamelen die ten minste twee cruciale aandachtsgebieden bestrijken: de doelwitten (door het identificeren van potentiële attack surfaces binnen de financiële entiteit) en de bedreigingen (door het identificeren van relevante dreigingsactoren en waarschijnlijke dreigingsscenario's). Om ervoor te zorgen dat de aanbieder van dreigingsinformatie de relevante bedreigingen voor de financiële entiteit in aanmerking neemt, moeten de testers, het *control team* en de testmanagers feedback geven over het ontwerprapport inzake dreigingsinformatie. Indien beschikbaar, kan de aanbieder van dreigingsinformatie een door de TLPT-autoriteit voor de financiële sector van een lidstaat verstrekt algemeen dreigingslandschap gebruiken als basis voor het nationale dreigingslandschap. Voortgaande op de toepassing van het TIBER-EU Framework neemt het proces van het verzamelen van dreigingsinformatie doorgaans ongeveer vier weken in beslag.

(19) Om testers in de gelegenheid te stellen inzicht te krijgen in het document met de afbakening van de scope ("scoping-document") en in het Target Threat Intelligence Report (TTI-rapport) en deze nader te bestuderen met het oog op het definitief vastleggen van het testplan voor het red team, is het van essentieel belang dat de testers, voorafgaand aan de red-teamtestfase van de TLPT, van de aanbieder van dreigingsinformatie een uitvoerige toelichting op het Target Threat Intelligence Report en een analyse van mogelijke dreigingsscenario's ontvangen.

(20) Om testers in staat te stellen een realistische en omvattende test uit te voeren waarbij alle aanvalsfasen worden uitgevoerd en flags worden bereikt, moet er voldoende tijd worden uitgetrokken voor de actieve red-teamtestfase. Op basis van de ervaring die met het TIBER-EU Framework is opgedaan, moet de toegewezen tijd ten minste twaalf weken bedragen en moet deze tijd worden bepaald op basis van het aantal betrokken partijen, de scope van de TLPT, de hulpbronnen van de betrokken financiële entiteit of entiteiten, eventuele externe vereisten, en de beschikbaarheid van door de financiële entiteit verstrekte ondersteunende informatie.

(21) Tijdens de actieve red-teamtestfase moeten de testers een reeks tactieken, technieken en procedures inzetten om de live productiesystemen van de financiële entiteit adequaat te testen. Die tactieken, technieken en procedures moeten, in voorkomend geval, omvatten: *reconnaissance* (het verzamelen van zo veel mogelijk informatie over een doelwit), *weaponization* (het analyseren van informatie over de infrastructuur, faciliteiten en medewerkers, alsmede het voorbereiden van de specifiek op het doelwit gerichte operaties), *delivery* (de actieve lancering van de volledige aanval op het doelwit), *exploitation* (waarbij het doel van de testers is om de servers en netwerken van de financiële entiteit te compromitteren en het personeel ervan te exploiteren door middel van social engineering), *control and movement* (pogingen om vanuit gecompromitteerde systemen andere kwetsbare of hoogwaardige systemen binnen te dringen) en *actions on objectives* (verkrijgen van verdere toegang tot gecompromitteerde systemen en tot de doelinformatie en -data, zoals van tevoren overeengekomen in het testplan van het red team).

(22) Bij het uitvoeren van een TLPT moeten de testers de beschikbare tijd voor het uitvoeren van de aanval, de middelen en de ethische en wettelijke grenzen in acht nemen. Indien de testers niet naar de geprogrammeerde volgende fase van de aanval kunnen doorgaan, moet het *control team*, met instemming van de TLPT-autoriteit, incidentele ondersteuning verlenen in de vorm van zogenoemde "leg-ups". Leg-ups kunnen grofweg worden ingedeeld in informatie- en in toegang-leg-ups en kunnen bijvoorbeeld bestaan uit het verlenen van toegang tot ICT-systemen of interne netwerken om de test te kunnen voortzetten en de aandacht op de volgende aanvalsstappen te kunnen richten.

(23) Tijdens de actieve red teaming in de testfase moet, indien het nodig is om de TLPT, als laatste redmiddel in uitzonderlijke omstandigheden en wanneer alle alternatieve opties zijn uitgeput, te kunnen voortzetten, worden gebruikgemaakt van collaboratieve testwerkzaamheden waarbij zowel de testers als het blue team zijn betrokken. In het kader van een dergelijke beperkte purple teaming-oefening kunnen de volgende methoden worden gebruikt: *catch-and-release* (waarbij testers proberen de scenario's voort te zetten, gedetecteerd te worden en vervolgens het testen te hervatten), *war gaming* (met complexere scenario's om strategische besluitvorming te testen) of *collaborative proof-of-concept* (waarmee testers en blue-teamleden gezamenlijk specifieke beveiligingsmaatregelen, tools of technieken kunnen valideren in een gecontroleerde en coöperatieve omgeving).

(24) De TLPT moet worden gebruikt als een leerervaring om de digitale operationele weerbaarheid van financiële entiteiten te versterken. In dat verband voeren het blue team en de testers een replay van de aanval uit en evalueren zij de stappen die zijn gezet om te leren van de testervaring, in samenwerking met de testers. Daartoe, en om een adequate voorbereiding mogelijk te maken, moeten het red-team-testrapport en het blue-team-testrapport beschikbaar worden gesteld aan alle partijen die betrokken zijn bij de replay, voordat er enige replay plaatsvindt. Daarnaast moet er in de afsluitende fase een purple teaming-oefening worden uitgevoerd om de leerervaring te maximaliseren. Methoden die voor purple teaming in de afsluitende fase kunnen worden gebruikt, zijn onder meer discussies over alternatieve aanvalsscenario's, verkenning van alternatieve scenario's op live systemen, of het opnieuw verkennen van geplande scenario's op live systemen die de testers tijdens de testfase niet hebben kunnen voltooien of uitvoeren.

(25) Om de leerervaring van alle bij de TLPT betrokken partijen verder te verbeteren — ten behoeve van toekomstige tests — en om de digitale operationele weerbaarheid van financiële entiteiten te bevorderen, moeten de betrokken partijen elkaar feedback geven over het algemene proces en moeten zij met name identificeren welke activiteiten goed zijn verlopen of hadden kunnen worden verbeterd en welke aspecten van het TLPT-proces goed hebben gewerkt of vatbaar zijn voor verbetering.

(26) De in artikel 46 van Verordening (EU) 2022/2554 bedoelde bevoegde autoriteiten en, indien daarvan verschillend, de TLPT-autoriteiten moeten samenwerken om geavanceerde tests op basis van TLPT te integreren in de bestaande toezichtprocedures. In dat verband, en om te komen tot een gezamenlijk correct begrip van de TLPT-bevindingen en de wijze waarop deze moeten worden geïnterpreteerd, is het passend dat er, met name voor het samenvattende testrapport en de remediëringsplannen, een nauwe samenwerking tussen de bij de TLPT betrokken testmanagers en de verantwoordelijke toezichthouders tot stand wordt gebracht.

(27) Artikel 26, lid 8, eerste alinea, van Verordening (EU) 2022/2554 legt financiële entiteiten de verplichting op om bij iedere derde test externe testers in te huren. Indien financiële entiteiten zowel interne als externe testers opnemen in het team van testers, moet dat voor de toepassing van voornoemd artikel worden beschouwd als een TLPT die wordt uitgevoerd met interne testers.

(28) Deze verordening is gebaseerd op de ontwerpen van technische reguleringsnormen die bij de Commissie zijn ingediend door de Europese Bankautoriteit, de Europese Autoriteit voor verzekeringen en bedrijfspensioenen en de Europese Autoriteit voor effecten en markten (de Europese toezichthoudende autoriteiten — "ESA's"), in samenspraak met de Europese Centrale Bank.

(29) De ESA's hebben open publieke consultaties gehouden over de ontwerpen van technische reguleringsnormen waarop deze verordening is gebaseerd, hebben de mogelijke kosten en baten ervan geanalyseerd en het advies ingewonnen van de overeenkomstig artikel 37 van Verordening (EU) nr. 1093/2010 van het Europees Parlement en de Raad ([3]) opgerichte Stakeholdergroep bankwezen, van de overeenkomstig artikel 37 van Verordening (EU) nr. 1094/2010 van het Europees Parlement en de Raad ([4]) opgerichte Stakeholdergroep verzekeringen en herverzekeringen en Stakeholdergroep bedrijfspensioenen, en van de overeenkomstig artikel 37 van Verordening (EU) nr. 1095/2010 van het Europees Parlement en de Raad ([5]) opgerichte Stakeholdergroep effecten en markten.

(30) Overeenkomstig artikel 42, lid 1, van Verordening (EU) 2018/1725 van het Europees Parlement en de Raad ([6]) is de Europese Toezichthouder voor gegevensbescherming geraadpleegd, die op 20 augustus 2024 een advies heeft uitgebracht,

HEEFT DE VOLGENDE VERORDENING VASTGESTELD:

Artikel 1

Definities

Voor de toepassing van deze verordening wordt verstaan onder:

1) "*control team*": het team samengesteld uit personeelsleden van de te testen financiële entiteit en, indien relevant gelet op de scope van de TLPT, personeelsleden van haar derde aanbieders van diensten en andere partijen, dat de test beheert;

2) "leider van het *control team*" (control team lead): het personeelslid van de financiële entiteit dat in het kader van een bepaalde test verantwoordelijk is voor de uitvoering van alle TLPT-gerelateerde activiteiten voor de financiële entiteit;

3) "blue team": de personeelsleden van de financiële entiteit en, in voorkomend geval, personeelsleden van de derde aanbieders van diensten van de financiële entiteit en andere partijen die relevant worden geacht gelet op de scope van de TLPT, die het gebruik van netwerk- en informatiesystemen door een financiële entiteit verdedigen door haar beveiligingshouding (security posture) tegen gesimuleerde of reële aanvallen te handhaven en die niet op de hoogte zijn van de TLPT;

4) "blue-teamtaken": taken die over het algemeen door het blue team worden uitgevoerd, zoals het beheer van het Security Operation Center (SOC), ICT-infrastructuurdiensten, helpdeskdiensten en incidentmanagementdiensten op operationeel niveau;

5) "red team": de interne of externe testers die zijn ingehuurd voor of toegewezen aan een TLPT;

6) "purple teaming": een collaboratieve testactiviteit waarbij zowel de testers als het blue team betrokken zijn;

([3]) Verordening (EU) nr. 1093/2010 van het Europees Parlement en de Raad van 24 november 2010 tot oprichting van een Europese toezichthoudende autoriteit (Europese Bankautoriteit), tot wijziging van Besluit nr. 716/2009/EG en tot intrekking van Besluit 2009/78/EG van de Commissie (PB L 331 van 15.12.2010, blz. 12, ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

([4]) Verordening (EU) nr. 1094/2010 van het Europees Parlement en de Raad van 24 november 2010 tot oprichting van een Europese toezichthoudende autoriteit (Europese Autoriteit voor verzekeringen en bedrijfspensioenen), tot wijziging van Besluit nr. 716/2009/EG en tot intrekking van Besluit 2009/79/EG van de Commissie (PB L 331 van 15.12.2010, blz. 48, ELI: http://data.europa.eu/eli/reg/2010/1094/oj).

([5]) Verordening (EU) nr. 1095/2010 van het Europees Parlement en de Raad van 24 november 2010 tot oprichting van een Europese toezichthoudende autoriteit (Europese Autoriteit voor effecten en markten), tot wijziging van Besluit nr. 716/2009/EG en tot intrekking van Besluit 2009/77/EG van de Commissie (PB L 331 van 15.12.2010, blz. 84, ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

([6]) Verordening (EU) 2018/1725 van het Europees Parlement en de Raad van 23 oktober 2018 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de instellingen, organen en instanties van de Unie en betreffende het vrije verkeer van die gegevens, en tot intrekking van Verordening (EG) nr. 45/2001 en Besluit nr. 1247/2002/EG (PB L 295 van 21.11.2018, blz. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

7) "TLPT-autoriteit": een van de volgende instanties:

   a) de overeenkomstig artikel 26, lid 9, van Verordening (EU) 2022/2554 aangewezen enige overheidsinstantie in de financiële sector;

   b) de autoriteit in de financiële sector waaraan de uitoefening van sommige of alle TLPT-gerelateerde taken is gedelegeerd overeenkomstig artikel 26, lid 10, van Verordening (EU) 2022/2554;

   c) de in artikel 46 van Verordening (EU) 2022/2554 bevoegde autoriteiten;

8) "TLPT-cyberteam" of "TCT": de personeelsleden binnen de TLPT-autoriteiten die verantwoordelijk zijn voor TLPT-kwesties;

9) "testmanagers": personeelsleden die zijn aangewezen om leiding te geven aan de activiteiten van de TLPT-autoriteit voor een specifieke TLPT, teneinde de naleving van deze verordening te monitoren;

10) "aanbieder van dreigingsinformatie": de deskundigen die voor elke TLPT door de financiële entiteit zijn ingehuurd en die extern zijn aan de financiële entiteit en, in voorkomend geval, aan intragroepsaanbieders van ICT-diensten, en die voor de financiële entiteiten binnen de scope van een specifieke TLPT-oefening relevante gerichte dreigingsinformatie verzamelen en analyseren en daarop aansluitende relevante en realistische dreigingsscenario's ontwikkelen;

11) "TLPT-aanbieders": testers en aanbieders van dreigingsinformatie;

12) "leg-up": de bijstand of informatie die het *control team* verschaft aan de testers zodat dezen de uitvoering van een aanvalspad kunnen voortzetten wanneer zij zelf geen verdere vooruitgang meer kunnen boeken en er geen ander redelijk alternatief bestaat, bijvoorbeeld omdat er onvoldoende tijd of middelen beschikbaar zijn voor een bepaalde TLPT;

13) "aanvalspad": de route die de testers tijdens de actieve red-teamtestfase volgen om de voor een TLPT gespecificeerde flags te bereiken;

14) "flags": essentiële doelstellingen die de testers door middel van de test proberen te bereiken in de ICT-systemen die kritieke of belangrijke functies van een financiële entiteit ondersteunen;

15) "gevoelige informatie": informatie die gemakkelijk kan worden ingezet voor het uitvoeren van aanvallen op de ICT-systemen van de financiële entiteit, intellectueel eigendom, vertrouwelijke bedrijfsgegevens of persoonsgegevens, die rechtstreeks of indirect schade kunnen toebrengen aan de financiële entiteit en haar ecosysteem indien deze in handen van kwaadwillende actoren zouden vallen;

16) "pool": alle financiële entiteiten die deelnemen aan een gepoolde TLPT overeenkomstig artikel 26, lid 4, van Verordening (EU) 2022/2554;

17) "lidstaat van ontvangst": de lidstaat van ontvangst volgens het sectorale Unierecht dat op elke financiële entiteit van toepassing is;

18) "gezamenlijke TLPT": een TLPT, niet zijnde een gepoolde TLPT als bedoeld in artikel 26, lid 4, van Verordening (EU) 2022/2554, waarbij meerdere financiële entiteiten zijn betrokken die gebruikmaken van dezelfde intragroepsaanbieder van ICT-diensten of die tot dezelfde groep behoren en ICT-systemen delen.

Artikel 2

Identificatie van financiële entiteiten die TLPT moeten uitvoeren

1. TLPT-autoriteiten beoordelen of financiële entiteiten een TLPT moet uitvoeren, rekening houdende met de impact van die financiële entiteiten op de financiële sector, hun systemische karakter en hun ICT-risicoprofiel, op basis van alle hiernavolgende criteria:

a) impactgerelateerde factoren en systemisch karakter:

   i) de omvang van de financiële entiteit, bepaald aan de hand van de vraag of de financiële entiteit financiële diensten in een of meer lidstaten verricht en door de activiteiten van de financiële entiteit te vergelijken met die van andere financiële entiteiten die soortgelijke diensten verrichten;

   ii) de mate en de aard van de verwevenheid van de financiële entiteit met andere financiële entiteiten in de financiële sector in een of meer lidstaten;

   iii) het kritieke karakter of het belang van de diensten die de financiële entiteit aan de financiële sector verleent;

iv) de substitueerbaarheid van de diensten die de financiële entiteit verleent;

v) de complexiteit van het bedrijfsmodel van de financiële entiteit en de daarmee verband houdende diensten en processen;

vi) de vraag of de financiële entiteit deel uitmaakt van een groep die een systemisch karakter op Unieniveau of op nationaal niveau in de financiële sector heeft en ICT-systemen deelt;

b) ICT-risicofactoren:

i) het risicoprofiel van de financiële entiteit;

ii) het dreigingslandschap van de financiële entiteit;

iii) de mate waarin kritieke of belangrijke functies, of functies die deze functies ondersteunen, van de financiële entiteit afhankelijk zijn van ICT-systemen en -processen;

iv) de complexiteit van de ICT-architectuur van de financiële entiteit;

v) de ICT-diensten en -functies die door derde aanbieders van ICT-diensten worden ondersteund, en de hoeveelheid en het soort contractuele regelingen met derde aanbieders van ICT-diensten of intragroeps-aanbieders van ICT-diensten;

vi) de resultaten van door toezichthouders verrichte toetsingen die relevant zijn voor de beoordeling van de ICT-maturiteit van de financiële entiteit;

vii) de maturiteit van ICT-bedrijfscontinuïteitsplannen en ICT-respons- en herstelplannen;

viii) de maturiteit van de operationele ICT-beveiligingsdetectie en -mitigatiemaatregelen, met inbegrip van het vermogen om:

1) de ICT-infrastructuur van de financiële entiteit op permanente basis te monitoren;

2) ICT-gerelateerde gebeurtenissen in realtime te detecteren;

3) de in punt 2) bedoelde gebeurtenissen te analyseren;

4) tijdig en doeltreffend op de in punt 2) bedoelde gebeurtenissen te reageren;

ix) de vraag of de financiële entiteit deel uitmaakt van een groep die actief is in de financiële sector op Unieniveau of op nationaal niveau en ICT-systemen deelt.

Voor de toepassing van punt a), i), houdt de TLPT-autoriteit, voor zover mogelijk, rekening met de volgende factoren:

a) het marktaandeel van de financiële entiteit op Unieniveau en op nationaal niveau;

b) het scala aan activiteiten dat door de financiële entiteit wordt aangeboden;

c) het marktaandeel van de door de financiële entiteit verrichte diensten of van de activiteiten die op Unieniveau en op nationaal niveau worden verricht.

Voor de toepassing van punt a), v), houdt de TLPT-autoriteit, voor zover mogelijk, rekening met volgende factoren:

a) of de financiële entiteit meer dan één bedrijfsmodel hanteert;

b) de onderlinge verwevenheid van verschillende bedrijfsprocessen en de daarmee verband houdende diensten.

2. TLPT-autoriteiten leggen elk van de volgende financiële entiteiten de verplichting op om TLPT's uit te voeren, tenzij uit de in lid 1 bedoelde beoordeling ten aanzien van een financiële entiteit blijkt dat haar impact, de zorgen over de financiële stabiliteit met betrekking tot die financiële entiteit of haar ICT-risicoprofiel de uitvoering van een TLPT niet rechtvaardigen:

a) kredietinstellingen die voldoen aan een van de volgende voorwaarden:

i) de instelling is aangemerkt als mondiaal systeemrelevante instelling ("MSI") overeenkomstig artikel 131 van Richtlijn 2013/36/EU van het Europees Parlement en de Raad ([7]);

ii) de instelling is aangemerkt als andere systeemrelevante instelling ("ASI") overeenkomstig artikel 131 van Richtlijn 2013/36/EU;

iii) de instelling maakt deel uit van een MSI of van een ASI;

([7]) Richtlijn 2013/36/EU van het Europees Parlement en de Raad van 26 juni 2013 betreffende toegang tot het bedrijf van kredietinstellingen en het prudentieel toezicht op kredietinstellingen en beleggingsondernemingen, tot wijziging van Richtlijn 2002/87/EG en tot intrekking van de Richtlijnen 2006/48/EG en 2006/49/EG (PB L 176 van 27.6.2013, blz. 338, ELI: http://data.europa.eu/eli/dir/2013/36/oj).

b) betaalinstellingen die in elk van de twee kalenderjaren voorafgaand aan de beoordeling door de TLPT-autoriteit de drempelwaarde van 150 miljard EUR aan betalingstransacties zoals gedefinieerd in artikel 4, punt 5), van Richtlijn (EU) 2015/2366 van het Europees Parlement en de Raad ([8]) hebben overschreden;

c) instellingen voor elektronisch geld die in elk van de twee kalenderjaren voorafgaand aan de beoordeling door de TLPT-autoriteit ofwel de drempelwaarde van 150 miljard EUR aan betalingstransacties zoals gedefinieerd in artikel 4, punt 5), van Richtlijn (EU) 2015/2366 van het Europees Parlement en de Raad, ofwel de drempelwaarde van 40 miljard EUR aan uitstaand elektronisch geld hebben overschreden;

d) centrale effectenbewaarinstellingen;

e) centrale tegenpartijen;

f) handelsplatformen met een elektronisch handelssysteem die voldoen aan een van de volgende criteria:

i) het handelsplatform heeft het hoogste marktaandeel in termen van op nationaal niveau behaalde omzet, in elk van de twee kalenderjaren voorafgaand aan de beoordeling door de TLPT-autoriteit, wat betreft:

1) effecten zoals gedefinieerd in artikel 4, lid 1, punt 44), a), van Richtlijn 2014/65/EU van het Europees Parlement en de Raad ([9]);

2) effecten zoals gedefinieerd in artikel 4, lid 1, punt 44), b), van Richtlijn 2014/65/EU;

3) derivaten zoals gedefinieerd in artikel 2, lid 1, punt 29), van Verordening (EU) nr. 600/2014 van het Europees Parlement en de Raad ([10]);

4) gestructureerde financiële producten zoals gedefinieerd in artikel 2, lid 1, punt 28), van Verordening (EU) nr. 600/2014;

5) emissierechten zoals bedoeld in deel C, punt 11, van bijlage I bij Richtlijn 2014/65/EU;

ii) het handelsplatform heeft een marktaandeel in termen van op Unieniveau behaalde omzet, van meer dan 5 % in elk van de twee kalenderjaren voorafgaand aan de beoordeling door de TLPT-autoriteit, wat betreft:

1) aandelen in vennootschappen en andere met aandelen in vennootschappen, personenvennootschappen of andere entiteiten gelijk te stellen effecten, alsmede aandelencertificaten;

2) obligaties of andere schuldinstrumenten, alsmede certificaten betreffende dergelijke effecten;

3) derivaten zoals gedefinieerd in artikel 2, lid 1, punt 29), van Verordening (EU) nr. 600/2014;

4) gestructureerde financiële producten zoals gedefinieerd in artikel 2, lid 1, punt 28), van Verordening (EU) nr. 600/2014;

5) emissierechten zoals bedoeld in deel C, punt 11, van bijlage I bij Richtlijn 2014/65/EU;

([8]) Richtlijn (EU) 2015/2366 van het Europees Parlement en de Raad van 25 november 2015 betreffende betalingsdiensten in de interne markt, houdende wijziging van de Richtlijnen 2002/65/EG, 2009/110/EG en 2013/36/EU en Verordening (EU) nr. 1093/2010 en houdende intrekking van Richtlijn 2007/64/EG (PB L 337 van 23.12.2015, blz. 35, ELI: http://data.europa.eu/eli/dir/2015/2366/oj).

([9]) Richtlijn 2014/65/EU van het Europees Parlement en de Raad van 15 mei 2014 betreffende markten voor financiële instrumenten en tot wijziging van Richtlijn 2002/92/EG en Richtlijn 2011/61/EU (PB L 173 van 12.6.2014, blz. 349, ELI: http://data.europa.eu/eli/dir/2014/65/oj).

([10]) Verordening (EU) nr. 600/2014 van het Europees Parlement en de Raad van 15 mei 2014 betreffende markten in financiële instrumenten en tot wijziging van Verordening (EU) nr. 648/2012 (PB L 173 van 12.6.2014, blz. 84, ELI: http://data.europa.eu/eli/reg/2014/600/oj).

g) (her)verzekeringsondernemingen die voldoen aan alle volgende criteria:

i) hun bruto geboekte premies bedragen meer dan 1 500 000 000 EUR;

ii) hun technische voorzieningen bedragen meer dan 10 000 000 000 EUR;

iii) de totale activa van verzekeringsondernemingen die uitsluitend levensverzekeringsactiviteiten uitoefenen of zowel levens- als schadeverzekeringsactiviteiten uitoefenen, bedragen meer dan 3,5 % van de som van de totale activa, zoals gewaardeerd overeenkomstig artikel 75 van Richtlijn 2009/138/EG van het Europees Parlement en de Raad ([11]), van de in de lidstaat gevestigde (her)verzekeringsondernemingen;

Voor de toepassing van punt f), ii), wordt, indien het handelsplatform deel uitmaakt van een groep die ICT-systemen deelt of gebruikmaakt van dezelfde intragroepsaanbieder van ICT-diensten, de omzet van de effecten- en derivatencontracten op alle handelsplatformen die tot dezelfde groep behoren en in de Unie zijn gevestigd, in aanmerking genomen.

Voor de toepassing van punt g) identificeren de TLPT-autoriteiten een subset van alle (her)verzekeringsondernemingen aan de hand van de in punt g), i), ii) en iii), vastgestelde criteria. (Her)verzekeringsondernemingen die tot die subgroep behoren, moeten TLPT's uitvoeren indien zij tevens voldoen aan een de volgende criteria:

a) de bruto geboekte premie bedraagt meer dan 3 000 000 000 EUR;

b) de technische voorzieningen bedragen meer dan 30 000 000 000 EUR;

c) de totale activa bedragen meer dan 10 % van de som van de totale activa, zoals gewaardeerd overeenkomstig artikel 75 van Richtlijn 2009/138/EG, van de in de lidstaat gevestigde (her)verzekeringsondernemingen.

3. Indien meer dan één financiële entiteit die tot dezelfde groep behoort en ICT-systemen deelt, of indien meer dan één financiële entiteit die gebruikmaakt van dezelfde intragroepsaanbieder van ICT-diensten, voldoet aan de criteria van lid 2, beslissen de TLPT-autoriteiten van die financiële entiteiten, overeenkomstig artikel 16, lid 2, of de verplichting om TLPT's op individuele basis uit te voeren, relevant is voor die financiële entiteiten.

Indien de TLPT-autoriteit van de moederonderneming van een in de eerste alinea bedoelde groep van financiële entiteiten verschilt van de TLPT-autoriteiten van de financiële entiteiten van de groep, wordt die autoriteit door de TLPT-autoriteiten van de tot die groep behorende financiële entiteiten geraadpleegd over de vraag of uitvoering van een TLPT op individuele basis passend is.

Artikel 3

TCT en TLPT-testmanagers

1. Een TLPT-autoriteit wijst de verantwoordelijkheid voor de coördinatie van TLPT-gerelateerde activiteiten toe aan een TIBER-cyberteam ("TCT"). Een TCT bestaat uit testmanagers die zijn aangewezen om een individuele TLPT te overzien.

2. Voor elke test wijst de TLPT-autoriteit een testmanager en ten minste één plaatsvervangende testmanager aan.

3. De testmanagers monitoren of en zien erop toe dat wordt voldaan aan de vereisten van deze verordening.

([11]) Richtlijn 2009/138/EG van het Europees Parlement en de Raad van 25 november 2009 betreffende de toegang tot en uitoefening van het verzekerings- en het herverzekeringsbedrijf (Solvabiliteit II) (PB L 335 van 17.12.2009, blz. 1, ELI: http://data.europa.eu/eli/dir/2009/138/oj).

4. De testmanager deelt de contactgegevens van het TCT mee aan de financiële entiteit door middel van de in artikel 9, lid 1, bedoelde kennisgeving.

5. De TLPT-autoriteit neemt deel aan alle fasen van de TLPT.

Artikel 4

Organisatorische regelingen voor financiële entiteiten

1. Financiële entiteiten stellen een leider van het *control team* aan die verantwoordelijk is voor het dagelijkse beheer van de TLPT en voor de beslissingen en acties van het *control team*.

2. Financiële entiteiten stellen organisatorische en procedurele maatregelen vast om ervoor te zorgen dat:

a) de toegang tot informatie over geplande of lopende TLPT's op een need-to-know-basis wordt beperkt tot het *control team*, het leidinggevend orgaan, de testers, de aanbieder van dreigingsinformatie en de TLPT-autoriteit;

b) het *control team* overleg pleegt met de testmanagers voordat een lid van het blue team bij een TLPT wordt betrokken;

c) het *control team* in kennis wordt gesteld van elke ontdekking van de TLPT door personeelsleden van de financiële entiteit of personeelsleden van haar derde dienstenaanbieders; in geval van escalatie van de uit een ontdekking voortvloeiende incidentrespons, indien nodig, het *control team* die escalatie indamt;

d) regelingen voor de geheimhouding van de TLPT zijn ingevoerd, die van toepassing zijn op het personeel van de financiële entiteit, het personeel van de betrokken derde aanbieders van ICT-diensten, de testers en de aanbieder van dreigingsinformatie;

e) het *control team* op verzoek alle informatie met betrekking tot de TLPT verstrekt aan de testmanagers;

f) de bij de TLPT betrokken partijen, indien mogelijk, alleen met een codenaam naar de test verwijzen.

Artikel 5

Risicomanagement voor TLPT

1. Tijdens de in artikel 9 bedoelde voorbereidingsfase beoordeelt het *control team* de risico's die zijn verbonden aan het testen van live productiesystemen van kritieke of belangrijke functies van de financiële entiteit, met inbegrip van de potentiële impact op:

a) de financiële sector;

b) de financiële stabiliteit op Unieniveau of op nationaal niveau.

Het *control team* beoordeelt die impact gedurende de hele test.

2. Ten behoeve van de risicobeoordeling en het risicomanagement houdt het *control team* ten minste rekening met de onderstaande soorten risico's die verbonden zijn aan:

a) het aan de aanbieder van dreigingsinformatie en externe testers verlenen van toegang, indien van toepassing, tot gevoelige informatie betreffende de financiële entiteit;

b) het niet in overeenstemming zijn van de TLPT met Verordening (EU) 2022/2554 en met deze verordening indien dat niet in overeenstemming zijn resulteert in het niet afgeven van het in artikel 26, lid 7, van Verordening (EU) 2022/2554 bedoelde attest, zelfs indien die niet-overeenstemming is te wijten aan inbreuken op de vertrouwelijkheid van de TLPT of een gebrek aan ethisch gedrag;

c) escalatie van crises en incidenten;

d) de actieve red-teamfase, met inbegrip van risico's in verband met de onderbreking van kritieke activiteiten en de aantasting van data als gevolg van de activiteiten van de testers, en de potentiële impact daarvan op derden;

e) de activiteit van het blue team, met inbegrip van risico's in verband met de onderbreking van kritieke activiteiten en de aantasting van data als gevolg van de activiteiten van het blue team, en de potentiële impact op derden;

f) de onvolledige terugzetting van systemen die door de TLPT zijn aangetast.

Artikel 6

Risicomanagement voor gepoolde of gezamenlijke TLPT's

1. In het geval van een gezamenlijke TLPT of een gepoolde TLPT voert het *control team* van elke financiële entiteit zijn eigen risicobeoordeling uit en stelt het zijn eigen maatregelen inzake risicomanagement vast.

2. Het *control team* van de aangewezen financiële entiteit zoals bedoeld in artikel 16, lid 3, punt b), van deze verordening of van de overeenkomstig artikel 26, lid 4, van Verordening (EU) 2022/2554 aangewezen financiële entiteit, beoordeelt de risico's die zijn verbonden aan de betrokkenheid van meerdere financiële entiteiten bij de TLPT. De *control teams* van de betrokken financiële entiteiten werken samen met het *control team* van de aangewezen financiële entiteit om potentiële gezamenlijke risico's in kaart te brengen.

Artikel 7

Selectie van TLPT-aanbieders

1. Het *control team* neemt maatregelen om de aan de TLPT verbonden risico's te beheersen en zorgt er met name voor dat voor elke TLPT:

a) de aanbieder van dreigingsinformatie en externe testers het *control team* een gedetailleerd curriculum vitae en kopieën van certificeringen overleggen die, volgens erkende marktnormen, passend zijn voor de uitvoering van hun activiteiten;

b) de aanbieder van dreigingsinformatie en externe testers naar behoren en volledig zijn gedekt door passende beroepsaansprakelijkheidsverzekeringen, onder meer tegen het risico van fouten en nalatigheid;

c) de aanbieder van dreigingsinformatie ten minste drie referenties van eerdere opdrachten in het kader van penetratietests en red-teamtests overlegt;

d) de externe testers ten minste vijf referenties van eerdere opdrachten in verband met penetratietests en red-teamtests overleggen;

e) het aan de TLPT toegewezen personeel van de aanbieder van dreigingsinformatie:

i) bestaat uit ten minste één manager met ten minste vijf jaar ervaring op het gebied van dreigingsinformatie en ten minste één ander lid met ten minste twee jaar ervaring op het gebied van dreigingsinformatie;

ii) beschikt over een breed scala aan, en een passend niveau van, professionele kennis en vaardigheden, waaronder:

1) tactieken, technieken en procedures voor het verzamelen van inlichtingen;

2) geopolitieke, technische en sectorale kennis;

3) adequate communicatievaardigheden om het resultaat van de opdracht op heldere wijze te presenteren en er over te rapporteren;

iii) gezamenlijk heeft deelgenomen aan ten minste drie eerdere opdrachten op het gebied van dreigingsinformatie in het kader van penetratietests en red-teamtests;

iv) niet tegelijkertijd blue-teamtaken of andere diensten uitvoert die kunnen leiden tot een belangenconflict met betrekking tot de financiële entiteit, de derde aanbieder van ICT-diensten of een intragroepsaanbieder van ICT-diensten die betrokken is bij een TLPT waaraan dat personeel is toegewezen;

v) is gescheiden van en niet rapporteert aan personeel van dezelfde TLPT-aanbieder die externe testers voor dezelfde TLPT levert;

f) in geval van externe testers, het aan de TLPT toegewezen red team:

i) bestaat uit ten minste één manager, met ten minste vijf jaar ervaring op het gebied van penetratietests en red-teamtests, en ten minste twee andere testers, elk met ten minste twee jaar ervaring op het gebied van penetratietests en red-teamtests;

ii) beschikt over een breed scala aan en een passend niveau van professionele kennis en vaardigheden, waaronder kennis over de bedrijfsactiviteiten van de financiële entiteit, reconnaissance, risicomanagement, exploit development, fysieke penetratie, social engineering en kwetsbaarheidsanalyse, alsmede adequate communicatievaardigheden om het resultaat van de opdracht op heldere wijze te presenteren en te rapporteren;

iii) heeft gezamenlijk deelgenomen aan ten minste vijf eerdere opdrachten op het gebied van penetratietests en red-teamtests;

iv) niet in dienst is van, noch diensten verleent aan, een aanbieder van dreigingsinformatie die tegelijkertijd blue-teamtaken uitvoert voor een financiële entiteit, een derde aanbieder van ICT-diensten of een intragroepsaanbieder van ICT-diensten die bij de TLPT betrokken is;

v) is gescheiden van het personeel van dezelfde TLPT-aanbieder dat tegelijkertijd dreigingsinformatiediensten verleent voor dezelfde TLPT;

g) de testers en de aanbieder van dreigingsinformatie aan het einde van de test herstelprocedures uitvoeren, zoals het veilig verwijderen van informatie over wachtwoorden, credentials en andere geheime sleutels die tijdens de TLPT zijn gecompromitteerd, beveiligde communicatie met de financiële entiteiten van de gecompromitteerde accounts en het beveiligd verzamelen, opslaan, beheren en verwijderen van andere tijdens het testen verzamelde data;

h) de testers, naast de herstelprocedures aan het einde van de testwerkzaamheden als bedoeld in punt g), de volgende herstelprocedures uitvoeren:

i) commando- en controledeactivering;

ii) scope en datum van kill-switches;

iii) verwijderen van achterdeuren en andere malware;

iv) kennisgeving van mogelijke inbreuken;

v) procedures voor toekomstige terugzetting van back-ups, waarbij het kan gaan om tijdens de test geïnstalleerde malware of tools;

vi) monitoren van de activiteiten van het blue team en verstrekken van informatie aan het *control team* over mogelijke ontdekkingen;

i) testers en de aanbieder van dreigingsinformatie geen van de volgende activiteiten uitvoeren of daar aan deelnemen:

i) ongeoorloofde vernietiging van apparatuur van de financiële entiteit en van haar derde aanbieders van ICT-diensten, in voorkomend geval;

ii) ongecontroleerde wijziging van informatie en ICT-activa van de financiële entiteit en van haar derde aanbieders van ICT-diensten, in voorkomend geval;

iii) het doelbewust compromitteren van de continuïteit van kritieke of belangrijke functies van de financiële entiteit;

iv) het ongeoorloofde opnemen van systemen van buiten de scope;

v) ongeoorloofde openbaarmaking van testresultaten.

2. Het *control team* houdt de door de testers en de aanbieders van dreigingsinformatie overgelegde documentatie bij zodat kan worden aangetoond dat is voldaan aan het bepaalde in lid 1, punten a) tot en met f).

In uitzonderlijke omstandigheden kunnen financiële entiteiten externe testers en aanbieders van dreigingsinformatie inhuren die niet voldoen aan een of meer van de in lid 1, punten a) tot en met f), vastgestelde vereisten, op voorwaarde dat die financiële entiteiten passende maatregelen nemen om de aan de niet-naleving van die punten verbonden risico's te mitigeren, en die maatregelen te documenteren.

Artikel 8

Specifieke bepalingen inzake gepoolde of gezamenlijke tests

1. Indien meerdere overeenkomstig artikel 16, lid 2 of lid 4, geïdentificeerde financiële entiteiten betrokken zijn bij een gepoolde of gezamenlijke TLPT, volgt elke financiële entiteit, tenzij anders wordt besloten door de leidende TLPT-autoriteit, elk van de in de artikelen 9 tot en met 15 beschreven stappen.

2. Indien meerdere TLPT-autoriteiten betrokken zijn bij een gezamenlijke of gepoolde TLPT zoals bedoeld in artikel 16, lid 3, of artikel 16, lid 5, worden, tenzij in deze verordening anders is bepaald, verwijzingen in de artikelen 9 tot en met 15 naar de "TLPT-autoriteit" opgevat als een verwijzing naar de leidende TLPT-autoriteit voor die gezamenlijke of gepoolde TLPT.

Artikel 9

Voorbereidende fase

1. Een overeenkomstig artikel 26, lid 8, derde alinea, van Verordening (EU) 2022/2554 geïdentificeerde financiële entiteit initieert een TLPT na ontvangst van een kennisgeving van de TLPT-autoriteit dat er een TLPT moet worden uitgevoerd.

2. Een financiële entiteit dient binnen drie maanden na ontvangst van de in lid 1 bedoelde kennisgeving alle volgende informatie over de initiëring van de TLPT in bij de testmanagers:

a) een project charter, met een projectplan op hoofdlijnen, dat de in bijlage I vermelde informatie bevat;

b) de contactgegevens van de leider van het *control team*;

c) informatie over het voorgenomen gebruik van interne of externe testers, of beide, indien relevant overeenkomstig artikel 15;

d) informatie over de tijdens de TLPT te gebruiken communicatiekanalen;

e) de codenaam voor de TLPT.

3. Indien de in lid 2, punten a) tot en met e), bedoelde informatie volledig is en de geschiktheid en daadwerkelijke uitvoering van de TLPT waarborgt, valideert de TLPT-autoriteit de TLPT-initiëringsinformatie van de financiële entiteit en stelt zij de financiële entiteit daarvan in kennis.

4. Nadat de TLPT-initiëringsdocumenten zijn gevalideerd door de TLPT-autoriteit, zet de financiële entiteit een *control team* op dat de leider van het *control team* ondersteunt bij zijn of haar taken om:

a) de communicatiekanalen en -processen binnen het *control team*, met de testers en met de aanbieders van dreigingsinformatie te specificeren voor alle kwesties met betrekking tot de TLPT;

b) het leidinggevend orgaan van de financiële entiteit te informeren over de voortgang van de TLPT en de daaraan verbonden risico's;

c) op basis van inhoudelijke deskundigheid beslissingen te nemen gedurende de hele TLPT;

d) de TLPT uit te voeren in overeenstemming met deze verordening;

e) voor de TLPT de aanbieders van dreigingsinformatie te selecteren;

f) de externe testers, de interne testers, of beiden, te selecteren;

g) het scoping-document op te stellen.

5. Indien de TLPT-autoriteit van oordeel is dat de initiële samenstelling van het *control team* en eventuele latere wijzigingen daarvan adequaat zijn voor de uitvoering van de in lid 4 bedoelde taken, valideert de TLPT-autoriteit het *control team* en stelt zij de leider van het *control team* daarvan in kennis.

6. De financiële entiteit dient binnen zes maanden na ontvangst van de in lid 1 bedoelde kennisgeving van de TLPT-autoriteit een scoping-document in bij de testmanagers dat alle in bijlage II vermelde informatie bevat. Het leidinggevend orgaan van de financiële entiteit keurt dit scoping-document goed.

7. Financiële entiteiten nemen de volgende criteria in aanmerking om kritieke of belangrijke functies in de scope van de TLPT op te nemen:

a) het kritieke karakter of belang van de functie en de mogelijke impact ervan op de financiële sector en de financiële stabiliteit op Unieniveau en op nationaal niveau;

b) het belang van de functie voor de dagelijkse bedrijfsvoering van de financiële entiteit;

c) de inwisselbaarheid van de functie;

d) de verwevenheid met andere functies;

e) de geografische locatie van de functie;

f) de sectorale afhankelijkheid van andere entiteiten van die functie;

g) indien beschikbaar, dreigingsinformatie over de functie.

8. Het *control team* deelt de TLPT-initiëringsdocumenten en het scoping-document met de testers en de aanbieders van dreigingsinformatie zodra deze zijn gecontracteerd. Het *control team* informeert de testers en de aanbieders van dreigingsinformatie over het te volgen testproces.

9. De financiële entiteit ziet erop toe dat het inhuren of toewijzen van testers en aanbieders van dreigingsinformatie is afgerond vóór de aanvang van de testfase.

10. Vóór de aanvang van de testfase raadpleegt het *control team* de testmanagers over de TLPT-risicobeoordeling en over de maatregelen inzake risicomanagement. Het *control team* evalueert de risicobeoordeling of de maatregelen inzake risicomanagement indien de TLPT-autoriteit van oordeel is dat deze de risico's van de TLPT niet adequaat tegengaan.

11. Het *control team* beoordeelt of de aanbieders van dreigingsinformatie en de testers die zij bij de TLPT overwegen te betrekken, voldoen aan de vereisten van artikel 27 van Verordening (EU) 2022/2554 en aan artikel 7, lid 1, van deze verordening, en documenteert de uitkomst van die beoordeling. Het *control team* selecteert de aanbieders van dreigingsinformatie in overeenstemming met die beoordeling en met zijn risicomanagementpraktijken. Voordat met de geselecteerde aanbieders van dreigingsinformatie en met de externe testers contracten worden afgesloten, levert het *control team* aan de testmanagers het bewijs dat die aanbieders van dreigingsinformatie en testers voldoen aan de vereisten van artikel 27 van Verordening (EU) 2022/2554 en aan artikel 7, lid 1, van deze verordening. Het *control team* contracteert de geselecteerde aanbieders van dreigingsinformatie en externe testers niet indien de TLPT-autoriteit van oordeel is dat de geselecteerde aanbieders van dreigingsinformatie en externe testers niet voldoen aan de vereisten van artikel 27 van Verordening (EU) 2022/2554 of aan de vereisten van artikel 7, lid 1, van deze verordening, of aan aanvullende vereisten die voortvloeien uit nationale veiligheidswetgeving in overeenstemming met Unierecht, of indien de financiële entiteit niet voldoet aan artikel 7, lid 2, eerste alinea, van deze verordening, of indien de in artikel 7, lid 2, tweede alinea, van deze verordening bedoelde omstandigheden niet zijn vervuld.

12. Indien het scoping-document volledig is en de uitvoering van een passende en doeltreffende TLPT waarborgt, keurt de TLPT-autoriteit dat document goed en stelt zij de leider van het *control team* daarvan in kennis.

Artikel 10

Testfase: dreigingsinformatie

1. Na de goedkeuring van het scoping-document door de TLPT-autoriteit analyseert de aanbieder van dreigingsinformatie algemene en sectorspecifieke dreigingsinformatie die relevant is voor de financiële entiteit. Indien de TLPT-autoriteit een algemeen dreigingslandschap voor de financiële sector van een lidstaat heeft verstrekt, kan de aanbieder van dreigingsinformatie dat landschap gebruiken als basis voor het nationale dreigingslandschap. De aanbieder van dreigingsinformatie brengt cyberdreigingen en bestaande of potentiële kwetsbaarheden die de financiële entiteit betreffen, in kaart. Daarnaast verzamelt de aanbieder van dreigingsinformatie informatie over concrete, actionable en gecontextualiseerde doel- en dreigingsinformatie over de financiële entiteit en analyseert hij deze, onder meer door raadpleging van het *control team* en de testmanagers.

2. De aanbieder van dreigingsinformatie presenteert de relevante dreigingen en informatie over gerichte dreigingen en stelt de benodigde scenario's voor aan het *control team*, de testers en de testmanagers. De voorgestelde scenario's verschillen van elkaar wat betreft de geïdentificeerde dreigingsactoren en de daarbij behorende tactieken, technieken en procedures en zijn gericht op elke kritieke of belangrijke functie binnen de scope van de TLPT.

3. De leider van het *control team* selecteert ten minste drie scenario's om de TLPT uit te voeren op basis van alle volgende elementen:

a) de aanbeveling van de aanbieder van dreigingsinformatie en het dreigingsgestuurde karakter van elk scenario;

b) de input van de testmanagers;

c) de haalbaarheid van de uitvoering van de voorgestelde scenario's, gebaseerd op het deskundige oordeel van de testers;

d) de omvang, de complexiteit en het algemene risicoprofiel van de financiële entiteit, en de aard, de schaal en de complexiteit van haar diensten, activiteiten en operaties.

4. Maximaal één van de geselecteerde scenario's mag niet-dreigingsgestuurd zijn en gebaseerd zijn op een prospectieve en potentiële fictieve dreiging met een hoge voorspellende, anticiperende, opportunistische of prospectieve waarde gezien de verwachte ontwikkelingen van het dreigingslandschap ten aanzien van de financiële entiteit.

Bij gepoolde TLPT's omvat ten minste één scenario, ongeacht de scenario's die rechtstreeks zijn gericht op de kritieke of belangrijke functies van de financiële entiteiten die bij de test zijn betrokken, de onderliggende ICT-systemen, -processen en -technologieën van de derde aanbieder van ICT-diensten die de kritieke of belangrijke functies van de financiële entiteiten binnen de scope ondersteunen.

Indien de test een gezamenlijke TLPT betreft waarbij een intragroepsaanbieder van ICT-diensten is betrokken, omvat ten minste één scenario, ongeacht de scenario's die rechtstreeks zijn gericht op kritieke of belangrijke functies van de financiële entiteiten die bij de test zijn betrokken, de onderliggende ICT-systemen, -processen en -technologieën van de intragroepsaanbieder van ICT-diensten die de kritieke of belangrijke functies van de financiële entiteiten binnen de scope ondersteunen.

5. De aanbieder van dreigingsinformatie verstrekt het Target Threat Intelligence Report (TTI-rapport), met inbegrip van de overeenkomstig de leden 3 en 4 geselecteerde scenario's, aan het *control team*. Het rapport inzake dreigingsinformatie bevat de in bijlage III vermelde informatie.

6. Het *control team* legt het Target Threat Intelligence Report ter goedkeuring voor aan de testmanager. Indien het Target Threat Intelligence Report volledig is en de uitvoering van een doeltreffende TLPT waarborgt, keurt de TLPT-autoriteit het rapport met gerichte dreigingsinformatie goed en stelt zij de leider van het *control team* daarvan in kennis.

Artikel 11

Testfase: red-teamtest

1. Nadat de TLPT-autoriteit het Target Threat Intelligence Report heeft goedgekeurd, stellen de testers het testplan voor het red team op, dat de in bijlage IV vermelde informatie bevat. De testers gebruiken het scoping-document en het Target Threat Intelligence Report als basis voor het opstellen van de aanvalsscenario's.

2. De testers raadplegen het *control team*, de aanbieder van dreigingsinformatie en de testmanagers over het testplan voor het red team, met inbegrip van de communicatie-, procedurele en projectmanagementregelingen, de voorbereiding op en de use-cases voor activering van leg-ups, en de regelingen voor rapportage aan het *control team* en de testmanagers.

3. Indien het testplan voor het red team volledig is en de uitvoering van een doeltreffende TLPT waarborgt, keuren het *control team* en de TLPT-autoriteit het testplan voor het red team goed en stelt de TLPT-autoriteit de leider van het *control team* daarvan in kennis.

4. Na goedkeuring van het testplan voor het red team overeenkomstig lid 3 voeren de testers de TLPT uit tijdens de actieve red-teamtestfase.

5. De duur van de actieve red-teamtestfase is evenredig aan de scope van de TLPT, het aantal, de schaal, de activiteit en de complexiteit van de financiële entiteiten en derde aanbieders van ICT-diensten of intragroepsaanbieders van ICT-diensten die bij de TLPT zijn betrokken, en bedraagt hoe dan ook ten minste twaalf weken. Aanvalsscenario's kunnen sequentieel of gelijktijdig worden uitgevoerd. Het *control team*, de aanbieder van dreigingsinformatie, de testers en de testmanagers komen overeen wanneer de actieve red-teamtestfase eindigt.

6. Op voorwaarde dat het testplan voor het red team volledig blijft en de uitvoering van een doeltreffende TLPT mogelijk maakt, geven de leider van het *control team* en de testmanagers goedkeuring voor alle wijzigingen in het testplan na de vaststelling ervan, met inbegrip van het tijdschema, de scope, de doelwitsystemen of flags.

7. Gedurende de gehele actieve red-teamtestfase rapporteren de testers ten minste wekelijks aan het *control team* en de testmanagers over de voortgang bij de TLPT en blijft de aanbieder van dreigingsinformatie beschikbaar voor overleg en voor aanvullende dreigingsinformatie wanneer het *control team* daarom verzoekt.

8. Het *control team* verstrekt tijdig leg-ups die zijn ontworpen op basis van het testplan voor het red team. Leg-ups kunnen worden toegevoegd of aangepast na goedkeuring van het *control team* en de testmanagers.

9. In het geval dat testwerkzaamheden worden ontdekt door een personeelslid van de financiële entiteit of van haar derde aanbieders van ICT-diensten of intragroepsaanbieder van ICT-diensten, al naargelang, stelt het *control team*, in overleg met de testers en onverminderd lid 10, de testmanagers ter validatie maatregelen voor waarmee de TLPT kan worden voortgezet maar toch geheim kan worden gehouden.

10. In buitengewone omstandigheden die risico's veroorzaken van impact op data, schade aan activa en verstoring van kritieke of belangrijke functies, diensten of operaties van de financiële entiteit zelf, van haar derde aanbieders van ICT-diensten of intragroepsaanbieders van ICT-diensten, of verstoringen van haar tegenhangers of van de financiële sector, kan de leider van het *control team* de TLPT opschorten of, als laatste redmiddel, indien de voortzetting van de TLPT anders niet mogelijk is en met inachtneming van voorafgaande validatie door de TLPT-autoriteit, de TLPT voortzetten met behulp van een beperkte purple teaming-oefening. De duur van de beperkte purple teaming-oefening wordt meegeteld voor de minimumduur van twaalf weken van de actieve red-teamtestfase waarvan sprake in lid 5.

Artikel 12

Afsluitende fase

1. Na het einde van de actieve red-teamtestfase informeert de leider van het *control team* het blue team dat er een TLPT heeft plaatsgevonden.

2. Binnen vier weken na het einde van de actieve red-teamtestfase dienen de testers bij het *control team* een red-team-testrapport in dat de in bijlage V vermelde informatie bevat.

3. Het *control team* verstrekt het red-team-testrapport zonder onnodige vertraging aan het blue team en aan de testmanagers.

Op verzoek van de testmanagers bevat het in de eerste alinea bedoelde rapport geen gevoelige informatie.

4. Na ontvangst van het red-team-testrapport, en uiterlijk tien weken na het einde van de actieve red-teamtestfase, dient het blue team bij het *control team* een blue-team-testrapport in dat de in bijlage VI vermelde informatie bevat. Het *control team* verstrekt het blue-team-testrapport onverwijld aan de testers en aan de testmanagers.

Op verzoek van de testmanagers bevat het in de eerste alinea bedoelde rapport geen gevoelige informatie.

5. Uiterlijk tien weken na het einde van de actieve red-teamtestfase voeren het blue team en de testers een replay uit van de offensieve en defensieve acties die tijdens de TLPT zijn uitgevoerd. Het *control team* voert ook een purple teaming-oefening uit ten aanzien van kwesties die door zowel het blue team als de testers zijn geconstateerd, op basis van kwetsbaarheden die tijdens de test zijn geconstateerd en, in voorkomend geval, van punten die tijdens de actieve red-teamtestfase niet konden worden getest.

6. Na afloop van de replay- en purple teaming-oefeningen geven het *control team*, het blue team, de testers en de aanbieders van dreigingsinformatie elkaar feedback over het TLPT-proces. Ook de testmanagers kunnen feedback geven.

7. Zodra de TLPT-autoriteit de leider van het *control team* ervan in kennis heeft gesteld dat zij heeft geoordeeld dat het blue-team-testrapport en het red-team-testrapport de in de bijlagen V en VI vermelde informatie bevatten, dient de financiële entiteit binnen acht weken het in artikel 26, lid 6, van Verordening (EU) 2022/2554 bedoelde rapport met een samenvatting van de relevante bevindingen van de TLPT, dat de in bijlage VII vermelde elementen bevat, ter goedkeuring in bij de TLPT-autoriteit.

Op verzoek van de TLPT-autoriteit bevat het in de eerste alinea bedoelde rapport geen gevoelige informatie.

Artikel 13

Remediëringsplan

1. Binnen acht weken na de in artikel 12, lid 7, van deze verordening bedoelde kennisgeving verstrekt de financiële entiteit de in artikel 26, lid 6, van Verordening (EU) 2022/2554 bedoelde remediëringsplannen en documentatie aan de TLPT-autoriteit en, indien daarvan verschillend, aan de bevoegde autoriteit van de financiële entiteit.

2. Het in lid 1 bedoelde remediëringsplan omvat voor elke bevinding die in het kader van de TLPT is gedaan:

a) een beschrijving van de vastgestelde tekortkomingen;

b) een beschrijving van de voorgestelde remediërende maatregelen en van de prioritering en de verwachte voltooiing van die maatregelen, met inbegrip van, in voorkomend geval, maatregelen om de identificatie-, beschermings-, detectie- en responscapaciteiten te verbeteren;

c) een root cause analysis;

d) de personeelsleden of de functies van de financiële entiteit die verantwoordelijk zijn voor de uitvoering van de voorgestelde remediërende maatregelen of verbeteringen;

e) de risico's die zijn verbonden aan de niet-uitvoering van de in punt b) bedoelde maatregelen en, in voorkomend geval, de risico's die zijn verbonden aan de uitvoering van die maatregelen.

Artikel 14

Attest

1. Het in artikel 26, lid 7, van Verordening (EU) 2022/2554 bedoelde attest bevat de in bijlage VIII vermelde informatie.

2. Indien bij een TLPT meerdere TLPT-autoriteiten betrokken zijn geweest, verstrekt de leidende TLPT-autoriteit het in artikel 26, lid 7, van Verordening (EU) 2022/2554 bedoelde attest aan de geteste financiële entiteiten.

Artikel 15

De inzet van interne testers

1. Financiële entiteiten stellen alle volgende regelingen vast voor het inzetten van interne testers:

a) de vaststelling en implementering van een beleid voor het beheer van interne testers in een TLPT;

b) maatregelen die moeten voorkomen dat het inzetten van interne testers voor het uitvoeren van een TLPT de algemene verdedigings- of weerbaarheidscapaciteiten van de financiële entiteit bij ICT-incidenten negatief beïnvloedt of aanzienlijke impact heeft op de beschikbaarheid van middelen voor ICT-taken tijdens een TLPT;

c) maatregelen om ervoor te zorgen dat interne testers de beschikking hebben over voldoende middelen en capaciteiten om een TLPT uit te voeren.

Het in punt a) bedoelde beleid:

a) omvat criteria om de geschiktheid, bekwaamheid en potentiële belangenconflicten van de interne testers te beoordelen en de managementverantwoordelijkheden in het testproces te specificeren;

b) wordt gedocumenteerd en wordt periodiek herzien;

c) voorziet erin dat het interne testteam bestaat uit een testleider en ten minste twee andere leden;

d) vereist dat alle leden van het testteam gedurende de voorgaande twaalf maanden in dienst zijn geweest bij de financiële entiteit of bij een intragroepsaanbieder van ICT-diensten;

e) omvat bepalingen inzake het opleiden van interne testers voor het uitvoeren van penetratietests en red-teamtests.

2. Indien een TLPT-autoriteit het inzetten van interne testers goedkeurt overeenkomstig artikel 27, lid 2, punt a), van Verordening (EU) 2022/2554, houdt de TLPT-autoriteit rekening met de vereisten van artikel 7, lid 1, van deze verordening.

3. Bij het inzetten van interne testers zorgt de financiële entiteit ervoor dat zulks in de volgende documenten wordt vermeld:

a) de in artikel 9 bedoelde testinitiëringsinformatie;

b) het in artikel 12, lid 2, bedoelde red-team-testrapport;

c) het in artikel 26, lid 6, van Verordening (EU) 2022/2554 bedoelde rapport met een samenvatting van de relevante bevindingen van de TLPT.

4. Testers die in dienst zijn bij een intragroepsaanbieder van ICT-diensten, worden beschouwd als interne testers van de financiële entiteit.

Artikel 16

Samenwerking en wederzijdse erkenning

1. Voor het uitvoeren van een TLPT op een financiële entiteit die diensten in meer dan één lidstaat verricht, al dan niet via een bijkantoor, doet de TLPT-autoriteit van die entiteit het volgende:

a) zij bepaalt welke TLPT-autoriteiten in lidstaten van ontvangst bij de test betrokken zullen worden, mede op basis van de vraag of een of meer kritieke of belangrijke functies worden uitgeoefend in, of gedeeld tussen, lidstaten van ontvangst;

b) zij stelt de overeenkomstig punt a) geïdentificeerde TLPT-autoriteiten in kennis van het besluit om een TLPT op de financiële entiteit uit te voeren;

c) zij leidt als TLPT-autoriteit van de financiële entiteit de TLPT, tenzij anders wordt overeengekomen door de TLPT-autoriteiten.

De TLPT-autoriteiten van de lidstaten van ontvangst kunnen binnen twintig werkdagen na ontvangst van de informatie over een toekomstige uitvoering van een TLPT ofwel blijk geven van hun belangstelling om de TLPT te volgen als waarnemer, ofwel een testmanager aanwijzen voor deelname aan de TLPT. De leidende TLPT-autoriteit verstrekt alle TLPT-autoriteiten die als waarnemers bij de TLPT optreden het scoping-document, het samenvattende rapport van de test, het remediëringsplan en het attest.

De leidende TLPT-autoriteit coördineert alle deelnemende TLPT-autoriteiten gedurende de hele test en neemt alle besluiten die nodig zijn voor een passende en doeltreffende uitvoering van de TLPT. De leidende TLPT-autoriteit kan een maximumaantal deelnemende TLPT-autoriteiten vaststellen wanneer de efficiënte uitvoering van de TLPT anders in het gedrang zou kunnen komen.

2. Indien een financiële entiteit gebruikmaakt van dezelfde intragroepsaanbieder van ICT-diensten als in andere lidstaten gevestigde financiële entiteiten, of tot een groep behoort en ICT-systemen deelt met in andere lidstaten gevestigde financiële entiteiten van dezelfde groep, neemt de TLPT-autoriteit van die financiële entiteit contact op met de TLPT-autoriteiten van de andere financiële entiteiten die gebruikmaken van dezelfde intragroepsaanbieder van ICT-diensten of die als onderdeel van de groep ICT-systemen delen, en beoordeelt zij samen met hen de haalbaarheid en geschiktheid van het uitvoeren van een gezamenlijke TLPT ten aanzien van de financiële entiteit. Indien zulks voor de financiële entiteiten en voor de TLPT-autoriteiten kan leiden tot een vermindering van de kosten en de te gebruiken middelen, heeft een gezamenlijke TLPT de voorkeur boven een individuele TLPT, op voorwaarde dat de deugdelijkheid en doelmatigheid van de testwerkzaamheden niet in het gedrang komen.

3. Voor het uitvoeren van een gezamenlijke TLPT:

a) komen de TLPT-autoriteiten van de financiële entiteiten overeen welke financiële entiteit wordt aangewezen voor het uitvoeren van een TLPT, gelet op de groepsstructuur en op de efficiëntie van de test;

b) leidt de TLPT-autoriteit van de overeenkomstig punt a) aangewezen financiële entiteit de TLPT, tenzij anders wordt overeengekomen door de TLPT-autoriteiten van de financiële entiteiten die aan de gezamenlijke TLPT deelnemen;

c) kunnen de TLPT-autoriteiten van de andere financiële entiteiten dan de aangewezen financiële entiteit onder leiding van wier TLPT-autoriteit de gezamenlijke TLPT zal worden uitgevoerd, ofwel blijk geven van hun belangstelling om de TLPT te volgen als waarnemer, ofwel een testmanager voor die TLPT aanwijzen.

De leidende TLPT-autoriteit coördineert alle TLPT-autoriteiten die bij de gezamenlijke TLPT betrokken zijn, en neemt alle besluiten die nodig zijn voor een deugdelijke en doeltreffende uitvoering van deze TLPT.

4. Indien een financiële entiteit voornemens is een gepoolde TLPT zoals bedoeld in artikel 26, lid 4, van Verordening (EU) 2022/2554 uit te voeren, waarbij mogelijkerwijs in andere lidstaten gevestigde financiële entiteiten betrokken zullen worden, neemt haar TLPT-autoriteit contact op met de TLPT-autoriteiten van de andere financiële entiteiten en beoordeelt deze samen met hen de haalbaarheid en geschiktheid van het uitvoeren van een gepoolde TLPT op die financiële entiteiten overeenkomstig artikel 26, lid 4, van Verordening (EU) 2022/2554.

5. Voor het uitvoeren van een gepoolde TLPT zoals bedoeld in artikel 26, lid 4, van Verordening (EU) 2022/2554:

a) komen de TLPT-autoriteiten van de financiële entiteiten overeen welke financiële entiteit wordt aangewezen om de gepoolde TLPT uit te voeren, rekening houdende met de door de derde aanbieder van ICT-diensten aan de financiële entiteiten verleende ICT-diensten en de efficiëntie van de test;

b) leidt de TLPT-autoriteit van de overeenkomstig punt a) aangewezen financiële entiteit de TLPT, tenzij anders wordt overeengekomen door de TLPT-autoriteiten van de financiële entiteiten die aan de gepoolde TLPT deelnemen;

c) kunnen de TLPT-autoriteiten van de andere financiële entiteiten dan de aangewezen financiële entiteit onder leiding van wier TLPT-autoriteit de gepoolde TLPT zal worden uitgevoerd, ofwel blijk geven van hun belangstelling om de TLPT te volgen als waarnemer, ofwel een testmanager voor die TLPT aanwijzen.

De leidende TLPT-autoriteit coördineert alle TLPT-autoriteiten die bij de gepoolde TLPT betrokken zijn, en neemt alle besluiten die nodig zijn voor een deugdelijke en doeltreffende uitvoering van deze TLPT.

6. Indien de TLPT-autoriteit van een financiële entiteit die een TLPT moet uitvoeren, verschilt van de in artikel 46 van Verordening (EU) 2022/2554 bedoelde bevoegde autoriteit van die financiële entiteit, delen die autoriteiten alle relevante informatie met betrekking tot alle TLPT-kwesties ten behoeve van de uitvoering van de TLPT of de uitvoering van hun taken in overeenstemming met die verordening.

Artikel 17

Inwerkingtreding

Deze verordening treedt in werking op de twintigste dag na die van de bekendmaking ervan in het *Publicatieblad van de Europese Unie*.

Deze verordening is verbindend in al haar onderdelen en is rechtstreeks toepasselijk in elke lidstaat.

Gedaan te Brussel, 13 februari 2025.

Voor de Commissie
De voorzitter
Ursula VON DER LEYEN

BIJLAGE I

Inhoud van het project charter (artikel 9, lid 2, punt a))

Informatie-element	Te verstrekken gegevens
Persoon verantwoordelijk voor het projectplan, d.w.z. de leider van het *control team*	Naam Contactgegevens
Testers	☐ intern ☐ extern ☐ beide
Overeenkomstig artikel 9, lid 2, punt d), en artikel 9, lid 4, punt a), geselecteerde communicatiekanalen, waaronder: a) de te gebruiken e-mailversleuteling b) de te gebruiken onlinedatarooms c) de te gebruiken instantmessaging	
Codenaam TLPT	
In voorkomend geval, kritieke of belangrijke functies die de financiële entiteit uitoefent in andere lidstaten	1. lijst van kritieke of belangrijke functies uitgeoefend in een andere lidstaat 2. voor elke kritieke of belangrijke functie: de lidstaat of lidstaten waar deze worden uitgeoefend
In voorkomend geval, de kritieke of belangrijke functies die worden ondersteund door derde aanbieders van ICT-diensten	3. lijst van kritieke of belangrijke functies ondersteund door derde aanbieders van ICT-diensten 4. voor elke functie: identificatie van de derde aanbieder van ICT-diensten
Verwachte uiterste datums voor de voltooiing van de/het:	
1) Voorbereidende fase, overeenkomstig artikel 9	jjjj-mm-dd
2) Testfase, overeenkomstig de artikelen 10 en 11	jjjj-mm-dd
3) Afsluitende fase, overeenkomstig artikel 12	jjjj-mm-dd
4) Remediëringsplan, overeenkomstig artikel 13	jjjj-mm-dd

BIJLAGE II

Inhoud van het scoping-document (artikel 9, lid 6)

1. Het scoping-document bevat een lijst van alle door de financiële entiteit geïdentificeerde kritieke of belangrijke functies.

2. Voor elke geïdentificeerde kritieke of belangrijke functie wordt de volgende informatie opgenomen:
   a) indien de kritieke of belangrijke functie niet binnen de scope van de TLPT valt: opgave van de redenen waarom deze niet is opgenomen;
   b) indien de kritieke of belangrijke functie binnen de scope van de TLPT valt:
      i) opgave van de redenen om de functie in de lijst op te nemen;
      ii) het (de) geïdentificeerde ICT-systeem(systemen) dat (die) deze kritieke of belangrijke functie ondersteunt (ondersteunen);
      iii) voor elk geïdentificeerd ICT-systeem:
         1. of het systeem is uitbesteed en zo ja, de naam van de derde aanbieder van ICT-diensten;
         2. de rechtsgebieden waarin het ICT-systeem wordt gebruikt;
         3. een beschrijving op hoofdlijnen van voorlopige flag(s), met vermelding van welke flag welk beveiligingsaspect van vertrouwelijkheid, integriteit, authenticiteit of beschikbaarheid betreft.

BIJLAGE III

Inhoud van het Target Threat Intelligence Report (artikel 10, lid 5)

Het Target Threat Intelligence Report (TTI-rapport) bevat informatie over elk van de volgende elementen:

1. De algehele scope van het onderzoek naar informatie, met inbegrip van ten minste het volgende:
   a) kritieke of belangrijke functies binnen de scope;
   b) de geografische locatie van die functie(s);
   c) gebruikte officiële EU-taal (-talen);
   d) de betrokken derde aanbieders van ICT-diensten;
   e) de periode waarin het onderzoek heeft plaatsgevonden.
2. Een algemene beoordeling van welke concrete, actionable informatie over de financiële entiteit te vinden is, waaronder:
   a) gebruikersnamen en wachtwoorden van werknemers;
   b) lookalike-domeinen die kunnen worden verward met officiële domeinen van de financiële entiteit;
   c) technische reconnaissance: kwetsbare of exploiteerbare software, systemen en technologieën;
   d) door werknemers op internet geposte informatie over de financiële entiteit die kan worden gebruikt voor een aanval;
   e) informatie die op het darkweb te koop is;
   f) alle andere relevante informatie die op internet of in openbare netwerken beschikbaar is;
   g) in voorkomend geval, informatie over fysieke targeting, met inbegrip van manieren om toegang te krijgen tot de bedrijfsruimten van de financiële entiteit.
3. Een analyse van de dreigingsinformatie die rekening houdt met het algemene dreigingslandschap en de specifieke situatie van de financiële entiteit, met inbegrip van ten minste:
   a) de geopolitieke omgeving;
   b) de economische omgeving;
   c) technologische trends en andere trends die verband houden met de activiteiten in de sector financiële diensten.
4. Dreigingsprofielen van kwaadwillende actoren (specifieke individuen/groepen of algemene categorieën) die zich op de financiële entiteit zouden kunnen richten, met inbegrip van de systemen van de financiële entiteit die kwaadwillende actoren het meest waarschijnlijk zullen compromitteren of aanvallen, mogelijke motieven, intenties en achterliggende gedachten om het potentiële doelwit uit te kiezen en mogelijke modi operandi van de aanvallers.
5. Dreigingsscenario's: ten minste drie end-to-end dreigingsscenario's voor de overeenkomstig punt 4 geïdentificeerde dreigingsprofielen met de hoogste scores voor de ernst van de dreiging. De dreigingsscenario's beschrijven het end-to-end aanvalspad en omvatten ten minste:
   a) één scenario dat voorziet in de gecompromitteerde beschikbaarheid van diensten, maar daar niet toe beperkt is;
   b) één scenario dat voorziet in de gecompromitteerde data-integriteit, maar daar niet toe beperkt is;
   c) één scenario dat voorziet in de gecompromitteerde vertrouwelijkheid van informatie, maar daar niet toe beperkt is.
6. In voorkomend geval, een beschrijving van het niet-dreigingsgestuurde scenario zoals bedoeld in artikel 10, lid 4.

BIJLAGE IV

Inhoud van het testplan voor het red team (artikel 11, lid 1)

Het testplan voor het red team bevat informatie over alle volgende elementen:

a) communicatiekanalen en -procedures;

b) de tactieken, technieken en procedures die wel en niet mogen worden gebruikt bij de aanval, met inbegrip van ethische grenzen voor social engineering;

c) de risicomanagementsmaatregelen die de testers in acht moeten nemen;

d) een beschrijving van elk scenario, met inbegrip van:

   i) de gesimuleerde dreigingsactor;

   ii) zijn intentie, motieven en doelen;

   iii) de functie(s) en het (de) ondersteunende ICT-systeem(-systemen) die het doelwit zijn;

   iv) de aspecten van vertrouwelijkheid, integriteit, beschikbaarheid en authenticiteit waarop de aanval gericht is;

   v) flags;

e) een gedetailleerde beschrijving van elk verwacht aanvalspad, waaronder de randvoorwaarden en mogelijke leg-ups door het *control team*, met inbegrip van termijnen voor de verstrekking en het mogelijke gebruik daarvan;

f) de planning van red teaming-werkzaamheden, met inbegrip van de tijdsplanning voor de uitvoering van elk scenario, ten minste opgesplitst aan de hand van de drie fasen die een tester respectievelijk doorloopt tijdens de testfase: binnendringen in ICT-systemen van de financiële entiteit, bewegen doorheen de ICT-systemen en uiteindelijk uitvoeren van acties op doelwitten, en ten slotte zich terugtrekken uit de ICT-systemen (IN-fase, THROUGH-fase en OUT-fase);

g) bijzonderheden van de infrastructuur van de financiële entiteit waarmee tijdens het testen rekening moet worden gehouden;

h) eventuele aanvullende informatie of andere middelen die de testers nodig hebben om de scenario's uit te voeren.

BIJLAGE V

Inhoud van het red-team-testrapport (artikel 12, lid 2)

Het red-team-testrapport bevat informatie over ten minste elk van de volgende elementen:

a) informatie over de uitgevoerde aanval, waaronder:

   i) de kritieke of belangrijke functies en geïdentificeerde ICT-systemen, -processen en -technologieën die de kritieke of belangrijke functie ondersteunen en die het doelwit van de aanval zijn, zoals geïdentificeerd in het testplan van het red team;

   ii) een samenvatting van elk scenario;

   iii) de bereikte en niet-bereikte flags;

   iv) met en zonder succes gevolgde aanvalspaden;

   v) de tactieken, technieken en procedures die met en zonder succes zijn gebruikt;

   vi) eventuele afwijkingen van het testplan voor het red team;

   vii) eventueel verleende leg-ups;

b) alle acties waarvan de testers wisten dat die door het blue team werden uitgevoerd om de aanval te reconstrueren en de effecten ervan te mitigeren;

c) ontdekte kwetsbaarheden en andere bevindingen, waaronder:

   i) een beschrijving van de kwetsbaarheden en andere bevindingen, met inbegrip van het kritieke karakter ervan;

   ii) een root cause analysis van succesvolle aanvallen;

   iii) aanbevelingen voor remediëring, met inbegrip van een indicatie van de remediëringsprioriteiten.

BIJLAGE VI

Inhoud van het blue-team-testrapport (artikel 12, lid 4)

Het blue-team-testrapport bevat informatie over ten minste elk van de volgende elementen:

1. voor elke door de testers in het red-team-testrapport beschreven aanvalsstap:
   a) een lijst van de gedetecteerde aanvalsacties;
   b) de log entries voor die detecties;
2. een beoordeling van de bevindingen en aanbevelingen van de testers;
3. door het blue team verzameld bewijs voor de aanval door de testers;
4. een root cause analysis van succesvolle aanvallen door de testers;
5. een lijst van lessons learned en het vastgestelde verbeterpotentieel;
6. een lijst met onderwerpen voor de purple teaming.

BIJLAGE VII

Inhoud van het rapport met een samenvatting van de relevante bevindingen van de TLPT (als bedoeld in artikel 26, lid 6, van Verordening (EU) 2022/2554)

Het samenvattende rapport van de test bevat informatie over ten minste elk van de elementen:

a) de betrokken partijen;

b) het projectplan;

c) de gevalideerde scope, met inbegrip van de beweegredenen voor de opneming of uitsluiting van kritieke of belangrijke functies en geïdentificeerde ICT-systemen, -processen en -technologieën die de kritieke of belangrijke functies uit de TLPT ondersteunen;

d) de geselecteerde scenario's en elke significante afwijking van het Target Threat Intelligence Report;

e) de uitgevoerde aanvalspaden en gebruikte tactieken, technieken en procedures;

f) de veroverde en niet-veroverde flags;

g) eventuele afwijkingen van het testplan voor het red team;

h) eventueel door het blue team gedetecteerde aanvalsacties;

i) purple teaming in de testfase, indien uitgevoerd, en de daarmee samenhangende omstandigheden;

j) eventueel gebruikte leg-ups;

k) de genomen risicomanagementsmaatregelen;

l) de geconstateerde kwetsbaarheden en andere bevindingen, waaronder over het kritieke karakter ervan;

m) een root cause analysis van succesvolle aanvallen;

n) een remediëringsplan op hoofdlijnen, waarin verbanden worden gelegd tussen de kwetsbaarheden en andere bevindingen, de root causes en de remediëringsprioriteiten;

o) de uit de ontvangen feedback getrokken lessen.

BIJLAGE VIII

Inhoud het TLPT-attest (als bedoeld in artikel 26, lid 7, van Verordening (EU) 2022/2554)

Het attest bevat ten minste alle volgende gegevens:

a) over de uitgevoerde TLPT:

  i) de begin- en einddatum van de TLPT;

  ii) de kritieke of belangrijke functies binnen de scope van de test;

  iii) indien van toepassing, informatie over kritieke of belangrijke functies binnen de scope van de test waarop de TLPT niet is uitgevoerd;

  iv) in voorkomend geval, andere financiële entiteiten die bij de TLPT betrokken waren;

  v) in voorkomend geval, de derde aanbieders van ICT-diensten die aan de TLPT hebben deelgenomen;

  vi) met betrekking tot testers:

    1. of er interne testers zijn ingezet;

    2. of artikel 5, lid 3, tweede alinea, is toegepast door de financiële entiteit;

  vii) de duur (in kalenderdagen) van de actieve red-teamtestfase;

b) indien meerdere TLPT-autoriteiten bij de TLPT betrokken waren: de andere TLPT-autoriteiten, en in welke hoedanigheid zij betrokken waren;

c) een lijst van de documenten die door de TLPT-autoriteit zijn onderzocht met het oog op de afgifte van het attest.